AXIS 230 MPEG-2 Network Camera

User's Manual

Intelligent Security & Fire

About This Document

This manual is intended for administrators and operators of the AXIS 230 MPEG-2 Network Camera, and is applicable for firmware release 3.10. Later versions of the document will be posted to the Axis Web site, as required.

Previous experience of networking will be of use when installing and using this product.

Safety Notices Used in This Manual

Caution! - Indicates a potential hazard that can damage the product.

Important! - Indicates a hazard that can seriously impair operation.
Do not proceed beyond any of the above notices until you have fully understood the implications.

Legal Considerations

Camera surveillance may be prohibited by laws that vary from country to country. Check the laws in your local region before using the AXIS 230 for surveillance.

The AXIS 230 uses MPEG-2 compression, which is technology licensed by the MPEG Consortium. The AXIS 230 includes 3 viewer licenses. The installation of more than 3 instances of the viewer requires you to purchase further licenses. Please contact your Axis reseller.

Intellectual Property Rights

Axis AB has intellectual property rights relating to technology embodied in the product described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the patents listed at http://www.axis.com/patent.htm and one or more additional patents or pending patent applications in the US and other countries.

Electromagnetic Compatibility (EMC)

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Re-orient or relocate the receiving antenna. Increase the separation between the equipment and receiver. Connect the equipment to an outlet on a different circuit to the receiver. Consult your dealer or an experienced radio/TV technician for help. Shielded (STP) network cables must be used with this unit to ensure compliance with EMC standards.

USA - This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

Europe CE - The AXIS 230 fulfills the requirements for radiated emission according to limit B of EN55022:1998. This applies when using the internal microphone or an external line input, but not when using an external microphone.

Liability

Every care has been taken in the preparation of this manual. Please inform your local Axis office of any inaccuracies or omissions. Axis Communications AB cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. Axis Communications AB makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Axis Communications AB shall not be liable nor responsible for incidental or consequential damages in connection with the furnishing, performance or use of this material.

Trademark Acknowledgments

Acrobat, Adobe, Boa, Ethernet, IBM, Internet Explorer, LAN Manager, Linux, Macintosh, Microsoft, Netscape Navigator, OS/2, UNIX, Windows, WWW are registered trademarks of the respective holders. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Axis Communications AB is independent of Sun Microsystems Inc.

Axis Support Services

Visit the Axis Support Web at www.axis.com/techsup/

AXIS 230 MPEG-2 Network Camera User's Manual.
Revision 1.0
Part Number: 20443
Dated: November 2003
Copyright © Axis Communications AB, 2003

Intelligent Security & Fire

Table Of Contents

Safety Notice - Battery Replacement 5
Introduction 6
Features and Benefits 6
Applications 8
Product Description 9
AXIS 230 - Front 9
AXIS 230 - Rear Panel 9
Hardware Inventory 10
Installing the AXIS 230 11
Installation using AXIS IP Utility 11
Manual Installation with ARP and Ping 11
Client System Requirements 12
The AXIS Media Control (Viewing Client) 13
Accessing the AXIS 230 from Internet Explorer 14
Configuring audio equipment 14
Operating the AXIS 230 15
Accessing and logging on to the AXIS 230 15
Access from a browser 16
The Live View Page 16
The Setup Tools 17
Video Settings 18
Audio Settings 20
Live View Layout 20
Events and Event Types 21
Upload Servers 25
Notification Servers 26
Port Status & Devices 27
The System Options 29
Users 30
Firewall Settings 31
Date & Time 32
TCP/IP Network Settings 33
SMTP (email) Network Settings 35
RTP (Multicast) Settings 35
Ports & Devices 36
Maintenance 37

Intelligent Security & Fire

Support - Logs & Reports 37
The Factory Default Settings 38
Appendix A - Troubleshooting 39
Pinging Your IP Address 42
Appendix B - Updating the Firmware 43
Update via FTP 43
Emergency Recovery Procedure 43
Appendix C - Customizing The AXIS 230 45
Modifying the File System 45
Configuration via FTP 45
Custom Web Pages 46
Appendix D - Unit Connections 49
The D-Sub Connector 49
The Terminal Block 49
Connecting Pan/Tilt Devices 51
Controlling and Monitoring 52
Appendix E - Audio Settings 54
Appendix F - Technical Specifications 55
Appendix G - Bandwidth 57
The Video Quality Level 57
Video Quality vs. Bit Rate 57
Index 59
Glossary of Terms 62

Intelligent Security & Fire

Safety Notice - Battery Replacement

The AXIS 230 MPEG-2 Network Camera uses a 3.0V CR2032 Lithium battery as the power supply for its internal real-time clock (RTC). This battery will, under normal conditions, last for a minimum of 5 years. Low battery power affects the operation of the RTC, causing it to reset at every power-up.

The battery should not be replaced unless required!

If the battery does need replacing, please observe the following points:

Caution!

- Danger of Explosion if battery is incorrectly replaced!
- Replace only with the same or equivalent battery, as recommended by the manufacturer.
- Dispose of used batteries according to the manufacturer's instructions.

Intelligent Security & Fire

Introduction

The AXIS 230 MPEG-2 Network Camera combines the features of a high quality network camera containing a built-in zoom with the functionality of a powerful video server, thus providing video and audio streams over IP networks. With its day/night functionality, the AXIS 230 provides quality video 24 hours a day.

The AXIS 230 provides real-time compression and transmission of a DVD-quality MPEG-2 video and audio stream over TCP/IP networks. A video stream from the AXIS 230 using no audio requires approximately a third of the bandwidth required by a Motion-JPEG stream of equivalent quality.

When viewing multimedia content (video and audio) in a browser on a network, various technologies and protocols are employed to supply the content. The video and audio streams are transmitted either as unicast, where communication is between a single sender and a single recipient, or as multicast, which is communication between a single sender and multiple recipients. Multicasting is an excellent way to save on bandwidth.

The AXIS 230 is a complete hardware and software solution that includes all the required networking connectivity for distributing multimedia content over the network. The built-in web server provides its own application page for direct viewing of the video stream, as well as full web-based control of the management and configuration functions. All of this can be accessed from a browser over the network.

The AXIS 230 MPEG-2 Network Camera

Features and Benefits

Powerful Camera Features - The AXIS 230 is based on a color camera block that includes a built-in 18x optical zoom lens, and day/night functionality for low light conditions, including locations lit by IR-illumination. For Pan/Tilt control, the camera is equipped with built-in support for RS232/485 and comes complete with the main Axis PT drivers. For direct local monitoring, the camera is also equipped with an analog composite video output.

Intelligent Security & Fire

Superior Imaging - The MPEG-2 video stream can be viewed on a LAN by up to 3 standard (unicast) clients, or by unlimited numbers of multicast clients. Full frame rate (25/30 frames per second) is assured, provided the required bandwidth is available. Four different image resolutions up to 720x576 (PAL) / 520x480 (NTSC) are available, and the video quality is configurable to 7 different levels. Each client (unicast or multicast) viewing the media stream requires its own license. Further licenses may be purchased from your reseller.

Audio functionality - The AXIS 230 supports uni-directional audio, from the camera to the viewer and is supplied with an integrated mono microphone. Also provided is an audio input, for connecting an external microphone or other source producing an amplified signal. The Audio Level alarm will alert remote operators in the event that sound is detected above a user-defined level.

Event functionality - Events can be triggered via either of the two alarm inputs, or via the Audio Level Alarm. The actions preformed by events are configured via the settings in the web interface, and can include the remote storage of MPEG-2 video recordings to FTP servers, and/or the activation of external devices through the available relay output. It is also possible to enable a pre-alarm video buffer, allowing up to 1 minute of video to be buffered in the server and transmitted when the event occurs. Users can also be notified of events by email.

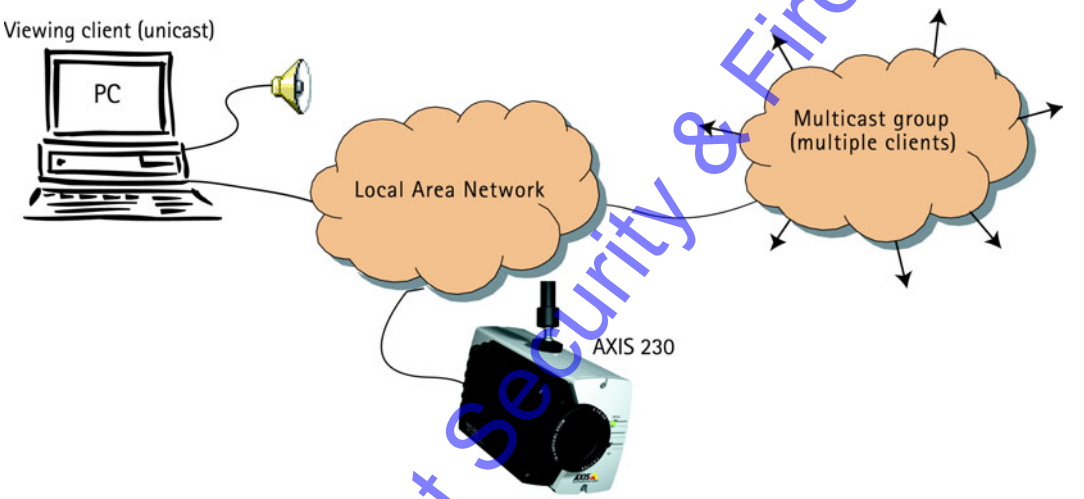
Security - Multi-user and multi-level password protection. Administrators can create and modify accounts for authorized users, as well as allow anonymous viewing. The built-in firewall provides IP address filtering, thus preventing unauthorized access.

Intelligent Security & Fire

Applications

The AXIS 230 MPEG-2 Network Camera can be used in a wide range of surveillance and monitoring applications, and is the perfect choice where an application requires a high-quality video and audio stream to be distributed at a fixed frame rate over a local area network (LAN). The AXIS 230 can also upload video sequences to FTP servers.

With direct access from your browser, you can view live video, and manage and control the camera at any time, from anywhere on the network.



The AXIS 230 is designed to meet user requirements for applications such as:

- Traffic monitoring
- Airport security
- Casino monitoring
- LAN-based remote learning

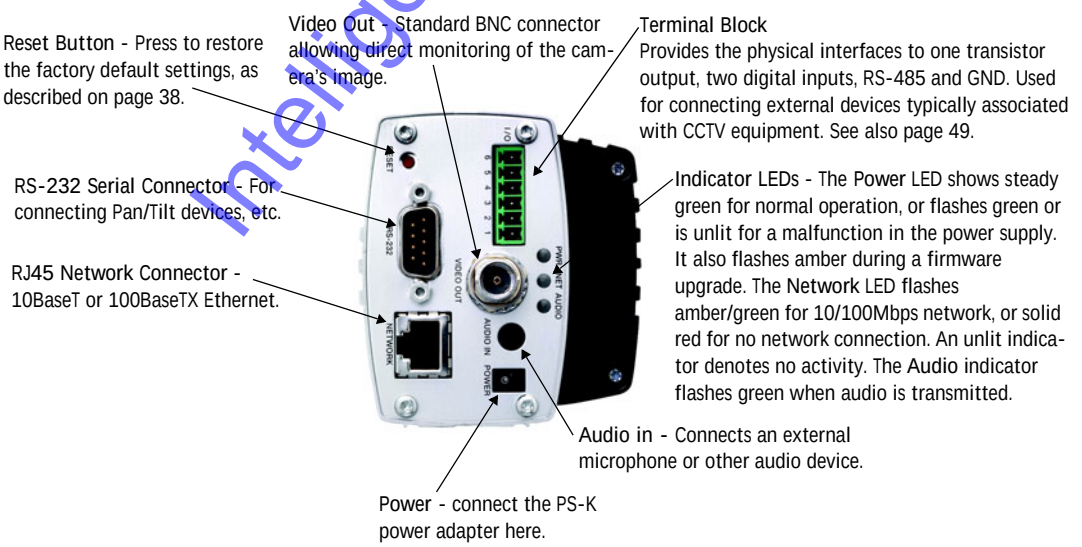
Intelligent Security & Fire

Product Description

Read the following information to familiarize yourself with the AXIS 230, making particular note of where the connectors and indicators are located.

AXIS 230 - Front

AXIS 230 - Rear Panel


Reset Button - Press to restore the factory default settings, as described on page 38.
Video Out - Standard BNC connector allowing direct monitoring of the camera's image.
Terminal Block
Provides the physical interfaces to one transistor output, two digital inputs, RS-485 and GND. Used for connecting external devices typically associated with CCTV equipment. See also page 49.
RS-232 Serial Connector - For connecting Pan/Tilt devices, etc.
Indicator LEDs - The Power LED shows steady green for normal operation, or flashes green or is unlit for a malfunction in the power supply. It also flashes amber during a firmware upgrade. The Network LED flashes amber/green for 10/100Mbps network, or solid red for no network connection. An unlit indicator denotes no activity. The Audio indicator flashes green when audio is transmitted.
RJ45 Network Connector - 10BaseT or 100BaseTX Ethernet.
Audio in - Connects an external microphone or other audio device.
Power - connect the PS-K power adapter here.
RESET
RS-232
VIDEO OUT
I/O
NETWORK
AUDIO IN
POWER
PWR
NET
AUDIO

Intelligent Security & Fire

Hardware Inventory

Check the items supplied with your AXIS 230 against the following list:

Item	Title/Variant	Quantity	Notes
Network Camera	AXIS 230 MPEG-2 Network Camera	1	
Power Supply (PS-K)	Europe UK USA Japan Australia	1	
Camera stand		1	
Mounting bracket		1	Note that this is packed under the moulded insert containing the camera
Terminal Connectors		1	
License letter		1	
Warranty Document		1	
This Document	AXIS 230 Network Camera User's Manual	1	
Disk Media	AXIS Product CD 1.2 (or later)	1	

Note: The power supply for the AXIS 230 is country-specific. Please check the type you are using is correct.

Intelligent Security & Fire

Installing the AXIS 230

This section is intended for use by the product administrator. Operators and viewers should read *Operating the AXIS 230,* on page 15.

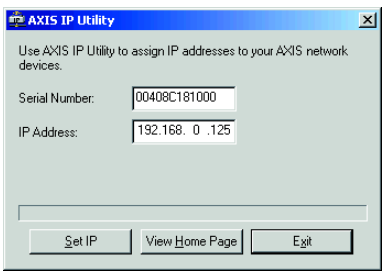
Installation using AXIS IP Utility

Important!

- Although it may be possible to use the AXIS 230's default IP address 192.168.0.90, please consult your network administrator to obtain a suitable IP address for your network/subnet.
- Although no special privileges are required for Windows XP Home, you will need Administrator privileges for Windows 2000 and XP Professional. UNIX systems require Root privileges.

AXIS IP Utility is a software application that quickly and simply installs an Axis device onto your local network. Download the latest version, free of charge, from www.axis.com

1. Connect an Ethernet cable to the AXIS 230 and attach it to the network.
2. Connect power to the camera.
3. Start AXIS IP Utility. The following window appears:

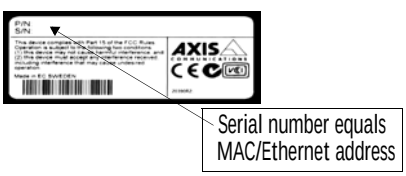


4. In the first field, enter the serial number found on the label on the underside of the unit (see the illustration below.)
5. Enter the IP address for the AXIS 230 and click Set IP. The utility now prompts you to restart the camera and then displays a message confirming that the IP address has been set. To view the camera's home page, click the button provided. Configure the remaining network parameters from the setup tools.

Manual Installation with ARP and Ping

As an alternative to the AXIS IP Utility, the AXIS 230 MPEG-2 Network Camera can be installed using the ARP and Ping commands, as described below.

1. Locate the label (see right) containing the product's serial number. You must know this to set the IP address.



2. Connect a network cable to the AXIS 230 and attach it to the network.
3. From a Windows computer on your network, open a Command Prompt and enter the commands shown below.

Intelligent Security & Fire

Example:

```
c:\WINNT>arp -s 192.168.0.125 00-40-8c-18-10-00
c:\WINNT>ping ping -l 408 -t 192.168.0.125
```

For Unix/Linux, enter the following: (note that you must be the root user.)

Example (for Linux):

```
>arp -s 192.168.0.125 00:40:8c:18:10:00 temp
>ping -s 408 192.168.0.125
```

Note: In some Unix/Linux systems, the arp command can be located in a directory that is not on the command path; e.g: /usr/sbin/arp

4. Now connect power to the camera. No more than 2 minutes should have elapsed since the ARP command was run. Text similar to the following is then displayed in the window:

```
c:\WINNT>arp -s 192.168.0.125 00-40-8c-18-10-00
c:\WINNT>ping -l 408 -t 192.168.0.125
Pinging 192.168.0.125 with 408 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.0.125: bytes=408 time<10ms TTL=64
Reply from 192.168.0.125: bytes=408 time<10ms TTL=64
```

5. Press Ctrl+C to stop Ping. Ensure that the Power Indicator is permanently lit and that the Network Indicator flashes intermittently. The IP address has been set. You can now access the camera and set other parameters from the setup tools. Please see page 14.

Client System Requirements

Client computers that will be viewing the video stream from the AXIS 230 should meet the following recommended hardware and software requirements:

- Pentium III (1.0 GHz processor or better) or AMD Athlon. 256 MB RAM.
- AGP graphics card with 32/64 MB video memory and support for DirectDraw®. Ensure that the latest available driver is used.
- Sound Card (PCI based.)
- Windows® 2000 or Windows XP (with latest Service Pack.)
- Internet Explorer 5.5 or higher (with latest Service Pack.)
- DirectX® (latest version.)
- A media player (only required for viewing saved MPEG-2 files.)

Intelligent Security & Fire

The AXIS Media Control (Viewing Client)

To view the video stream from the AXIS 230 in a browser, the AXIS Media Control must be installed. This is performed automatically the first time the camera is accessed from a browser. Simply accept the license agreement displayed in the setup window and the client will install. After the installation has completed, restart your computer, if required.

The AXIS Media Control employs MPEG-2 technology, the use of which is licensed by the MPEG Consortium.

Important!

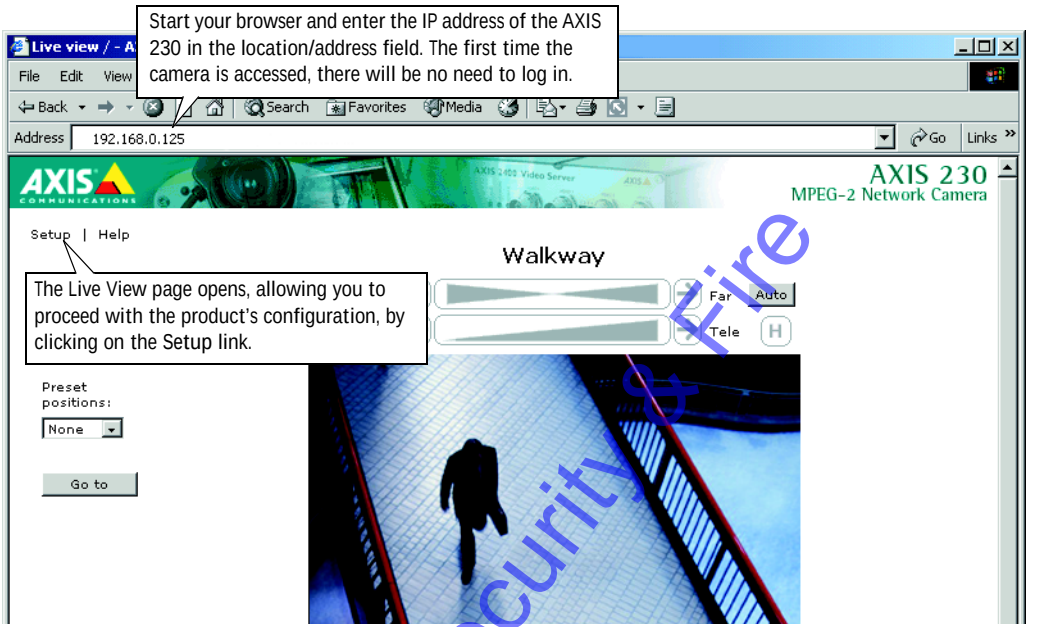
- The AXIS 230 employs MPEG-2 compression, which is technology licensed by the MPEG Consortium. 3 viewer licenses are included with the product. The installation of more than 3 instances of the viewer requires you to purchase further licenses. Please contact your Axis reseller.
- To allow the installation of the AXIS Media Control on your workstation, you must have administrator privileges. Your browser must also be set to allow the installation of signed ActiveX controls. This is the default setting in Internet Explorer.
- A viewing license may be used for multicast or unicast clients, but each individual client requires a separate license.
- No more than 3 unicast clients can view the video stream at any one time, no matter how many viewing licences are installed.

After the client is installed, there will be a new icon in the Windows Control Panel. Clicking on this icon opens the Control Applet for the AXIS Media Control, from where various settings can be changed. Please see the readme file included in the tool for more information.

The AXIS Media Control can be uninstalled from the Windows Control Panel.

Intelligent Security & Fire

Accessing the AXIS 230 from Internet Explorer


Start your browser and enter the IP address of the AXIS 230 in the location/address field. The first time the camera is accessed, there will be no need to log in.
Live view / - A
File Edit View
Back Search Favorites Media
Address 192.168.0.125
Go Links
AXIS
AXIS 230
MPEG-2 Network Camera
Setup | Help
The Live View page opens, allowing you to proceed with the product's configuration, by clicking on the Setup link.
Walkway
Far
Auto
Tele
H
Preset positions:
None
Go to

Important!

Upon delivery, the AXIS 230 is supplied with one pre-configured Administrator user name and password, set to *root* and *pass*, respectively. The Administrator password should be changed as soon as possible, to prevent unauthorized access to the setup tools and/or the video stream.

Configuring audio equipment

The internal microphone or other audio equipment should now be configured:

1. From the setup tools, open the Audio settings page and check the Enable box.
2. Select the input you connected your external equipment to (*external line* or *external mic*), or select *Internal Microphone*. Note that this is the *logical* connector. All of these options connect via the Audio In connector on the rear panel.
3. Some microphone types require their own (external) voltage supply to operate correctly. These types are condenser microphones and Electret microphones. If using one of these types of microphone, and it is not battery powered, check the box External Mic Power. This option should not be enabled when using a dynamic or battery powered microphone, as this will result in decreased sound quality.
4. Set the desired audio quality, and set the Mic Input Sensitivity according to your microphone. Click Save and then return to the Live View page to check that audio is available. See also the audio settings section on page 20.

Intelligent Security & Fire

Operating the AXIS 230

This section is intended mainly for system *Operators,* that is, personnel responsible for using the AXIS 230 as part of e.g. an integrated surveillance system or similar. Product *Administrators* will also find this section useful reading. The following topics are covered:

- accessing the AXIS 230 MPEG-2 Network Camera
- editing audio and video settings
- changing the layout of the Live View page
- adding and modifying event types and upload servers
- checking port and device status.

For more information on configuring the AXIS 230 at the Administrator level, please refer to *The System Options,* on page 29.

Accessing and logging on to the AXIS 230

The AXIS 230 allows several levels of access and generally requires the user to log on. The various access levels allow different degrees of control and some options/controls are not available at all levels.

An operator will have access to the camera's Live view page, as well as certain other functions and controls - in short, everything not included in the System Options, which are only available to administrators.

The only exception to the logon requirement is if the camera has been configured to allow anonymous viewing access and an anonymous user connects.

Important!

Your system administrator has installed the AXIS 230 on your network and tailored the functions of the system to meet your specific needs. Consequently, the examples provided here may differ from those displayed in your system. Any problems with your application should be referred to your system administrator.

Intelligent Security & Fire

Access from a browser

The video stream and the setup tools in the AXIS 230 can be accessed using Microsoft Internet Explorer 5.5 or higher on Windows 2000 or Windows XP.

Follow the instructions below to access your images:

1. Start Internet Explorer.
2. Enter the name or IP address of the AXIS 230 into the Address field:

Example!

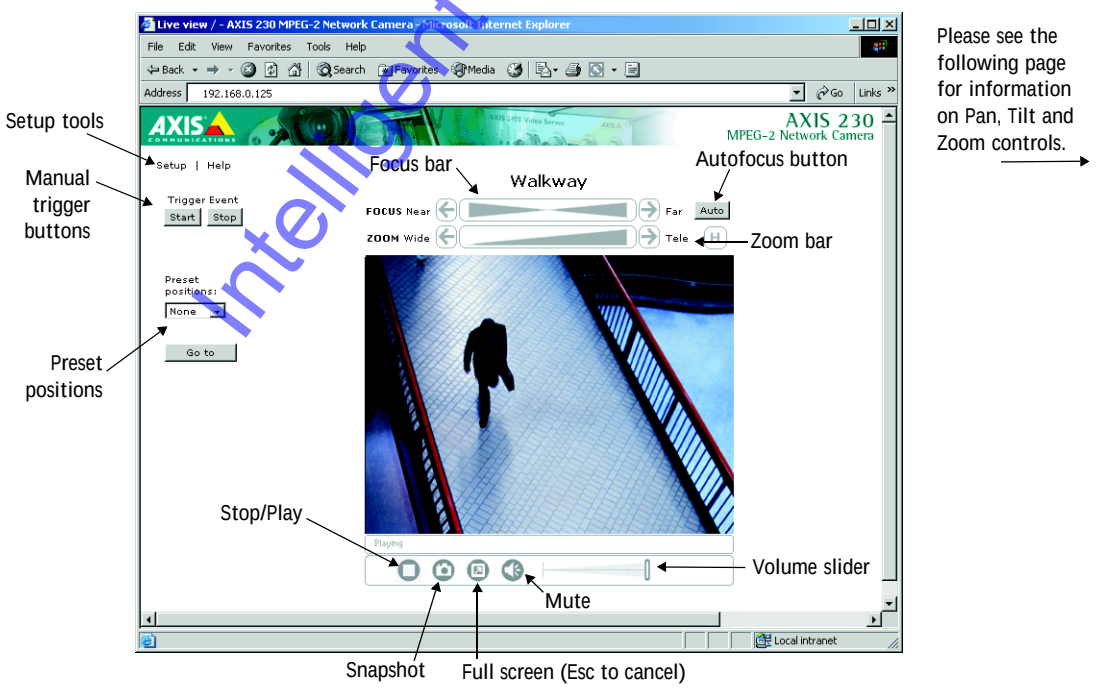
```
http://192.168.0.125/
```

The Live View page, similar to the example shown below, is now displayed.

Note: To view the MPEG-2 video stream in Microsoft Internet Explorer, the AXIS Media Control must be installed onto your computer. This will be performed automatically the first time the camera is accessed. Internet Explorer should be set to allow signed ActiveX controls.

The Live View Page

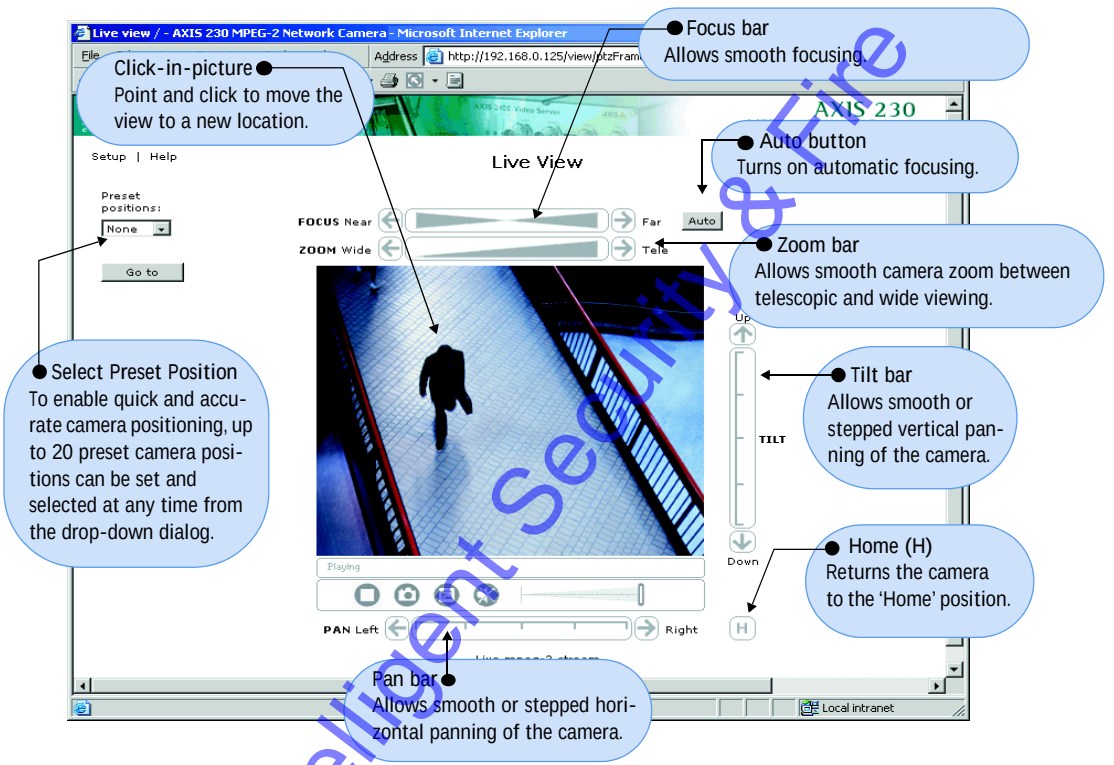
The page available to all user levels when accessing the AXIS 230 is known as the Live View page. This page displays a live MPEG-2 video stream, which can be viewed simultaneously by up to 3 unicast clients, or by many more multicast clients.



Intelligent Security & Fire

Positional Control of the Video Source

Pan/Tilt devices connected to the AXIS 230's ports can be controlled directly from the web interface, or by third-party applications. When using such a device, Pan and Tilt bars are automatically displayed, as shown in the example below. Note that the selected Pan/Tilt driver determines the actual layout of the controls. Other functions, not shown here, may also be available.



Intelligent Security & Fire

Notes: •Pan/Tilt controls can be disabled in the Live View layout settings and might not be available in the user interface.

•Clicking anywhere on a bar's gradient allows for a "smooth" adjustment; whereas clicking on the left or right arrows causes a stepped incremental change.

The Setup Tools

Clicking on the Setup link at the top left of the Live View page opens the Basic Configuration page, which provides links to the basic settings required by most systems. The settings found in the Basic Configuration section are described under the relevant section in the following pages.

Video Settings

The AXIS 230's video settings, as described below, may or may not need adjustment.

- Resolution - the available video resolutions for the AXIS 230 are listed in the table below. The exact resolution will depend on the modulation type - PAL or NTSC. See also the *Technical Specifications,* on page 55.

Resolution	NTSC	PAL
QCIF	160x112	160x144
CIF	352x240	352x288
2CIF	720x240	720x288
4CIF	720x480	720x576

Note: When using the resolution 2CIF, the image in Live View is rescaled to 4CIF. The image appears the same, but uses less bandwidth than 4CIF. When saving snapshots in 2CIF, these are saved at the original resolution of 720x240 (NTSC) / 720x288 (PAL).

- Color - Select either Color or Black & White. Black & White will provide sharper images at a lower bandwidth than Color.
- Quality level - This setting determines the quality of the video stream, which in turn affects the amount of bandwidth used. 1 is the lowest level and 7 the highest. See also *Bandwidth,* on page 57.
- White Balance - This can be described as the reference color against which all other colors in an image are compared. The white balancing system in the camera automatically detects white colors in any image and uses these intelligently as a reference for other colors. Note that the white balancing system will not operate effectively in certain situations. Problems generally occur if the image contains no white at all, or if the dominant color is something other than white. In these circumstances, using a fixed white balance mode is recommended. Please see the camera's online help for more information.
- Shutter speed - This parameter defines the exposure period for each image. Use a high shutter speed only if the image subject is expected to be moving quickly; otherwise, Auto or a slow speed will normally suffice.
- Brightness - Determine the brightness for your images in the range 0-15; where a low level setting produces darker images, and a high level produces brighter images. Select Auto to set automatic control, or set a value from 0 to 15, where 15 is the maximum brightness.
- Backlight compensation - To get good quality video of a subject in the foreground and when the background is strongly lit, the back-lighting must be compensated for. Set this to On.
- Sharpness - Defines a level of differentiation between light and dark areas within the image. Corresponding higher levels of sharpness provide for sharper images, but also cause the image compression to be more complex. Consequently, the file size of a sharp image can be significantly greater than an image that is less sharp. The setting may be made in the range 0-15.

Intelligent Security & Fire

- Max Digital Zoom - To prevent distortion of the video stream when zooming, set a maximum value for the digital zoom. This ensures that you always get video of a certain minimum defined quality.
- Focus Near Limit - This setting is useful when the camera is mounted e.g. behind glass in an outdoor enclosure. In certain circumstances, e.g. when rain or snow falls on the glass, the auto-focus function may attempt to refocus on this new element in the image. To prevent this phenomenon, set the focus near limit to a value greater than the distance at which disturbances are likely to occur.
- Mirror - To flip the image horizontally 180 degrees, set this to On.
- IR Illumination - If the camera is placed in a very dark location without lighting or is used at night, the autofocus function will not find anything to focus on and will repeatedly attempt to focus the camera, thus causing unnecessary wear on the focusing motor. Under normal circumstances, this is prevented by the built-in autofocus protection, but if using infrared (IR) illumination in a dark location, then the camera should behave as if the scene was lit normally, and the autofocus protection will not be necessary. Set the parameter to the correct setting for your application. Note that the AXIS 230 is intended for use in day and night situations, and will thus function well in very dark conditions, even when not using IR illumination.

Advanced Settings

The advanced settings allow the structure of the MPEG-2 video stream to be modified. The GOP (Group of Pictures) can take 3 forms - IBBP, IBP and IP. These forms describe the type of pictures included in the stream and also their internal order. An I-picture is a complete image, a P-image is the predicted difference between this image and a preceding I or P-picture, and a B-picture is a comparison with both earlier and later pictures.

Please note that changing this setting is likely to affect the amount of bandwidth required by the video stream, as well as the perceived latency. These settings should only be changed by experienced users.

Intelligent Security & Fire

Audio Settings

The AXIS 230 provides a fully synchronized audio stream at up to CD quality. The following settings are available:

- Quality - Select the bit rate and sample rate to use. Generally speaking, the higher the setting, the better the sound quality, but at the higher levels the difference might not be audible. The default value (128 Kbit/s) provides good quality sound.
- Input - Select the input to use for the audio input. The options are:

  Line - connects other audio input devices to the Audio In connector on the rear panel.

  Internal microphone - uses the built-in microphone located on the front of the camera.

  External microphone - connects a standard microphone to the Audio In connector.
- External Mic Power - Some microphone types require their own (external) supplied voltage to operate correctly. These are Condenser microphones and Electret microphones. If using a microphone of this type, and if it is not battery powered, check this box. This should not be enabled when using a dynamic or battery powered microphone, as sound quality may be impaired.
- Volume Settings - The Master volume control should not normally need any adjustment. However, if you are using an audio input device on the Line connector, and the audio level is unsatisfactory, then this level may need to be changed. The setting is configurable between -30 and 30 dB. If you need to configure the volume from the AXIS 230 to the same level as other wave sources originating from the PC, the Master volume control may be the only way to adjust this. This also depends on the sound card being used.
- Mic input sensitivity - This setting should be set according to the specifications for the external microphone. If the correct setting is used, there will be no need to adjust the Master volume level. The volume slider in the web interface will suffice for raising or lowering the volume when viewing the video stream. If you are unsure of the correct setting for your microphone, try both settings.

Live View Layout

The home page for the AXIS 230 MPEG-2 Video camera can be altered to your own requirements. Click the link to Live View Layout to open the Personal Settings.

Most of the features on the Live View page can be customized. For example, you can quickly change the background color and include your corporate logo.

Once you have enabled personal settings by checking the box, you can then change most aspects of the page. Simply select the item to use and then choose whether to use the default setting or to specify your own. For many of the items, selecting Own will also require you to specify the location for the resource, for example, the location of the background picture to use.

Intelligent Security & Fire

When you are satisfied with the new layout, click Save.

Note: Unchecking the *Show Setup* link will mean that the administration tools will then only be accessible by entering the *full address* to the tools into the browser's URL field, for example: http://172.21.1.200/operator/. Please make a note of the address for your camera, for future use.

Events and Event Types

The AXIS 230 MPEG-2 is capable of performing various actions when certain types of events occur. The terminology used to describe this is as follows:

- Event type - a defined set of parameters that specify how and when something will trigger an action.
- Event - an event that occurs while the system is running. Started by a trigger, it initiates an action, and is time-stamped and named.
- Action - what occurs when the event triggers. Examples are the upload of video to an FTP server, email notification, etc.
- Trigger - the circumstances that start an event. This could be e.g. a pre-programmed time or a signal from an external device, such as a door switch or a motion sensor.

Configuring Event Types

An event type is a set of parameters describing how and when the camera will perform certain actions. An event type may result in one single event, or it may result in many, depending on how often its preconditions are met. The most common kind of event type will trigger the upload of video to a specified destination. Other actions performed by event types can include the sending of e-mail, the activation of the output port and various types of event notification.

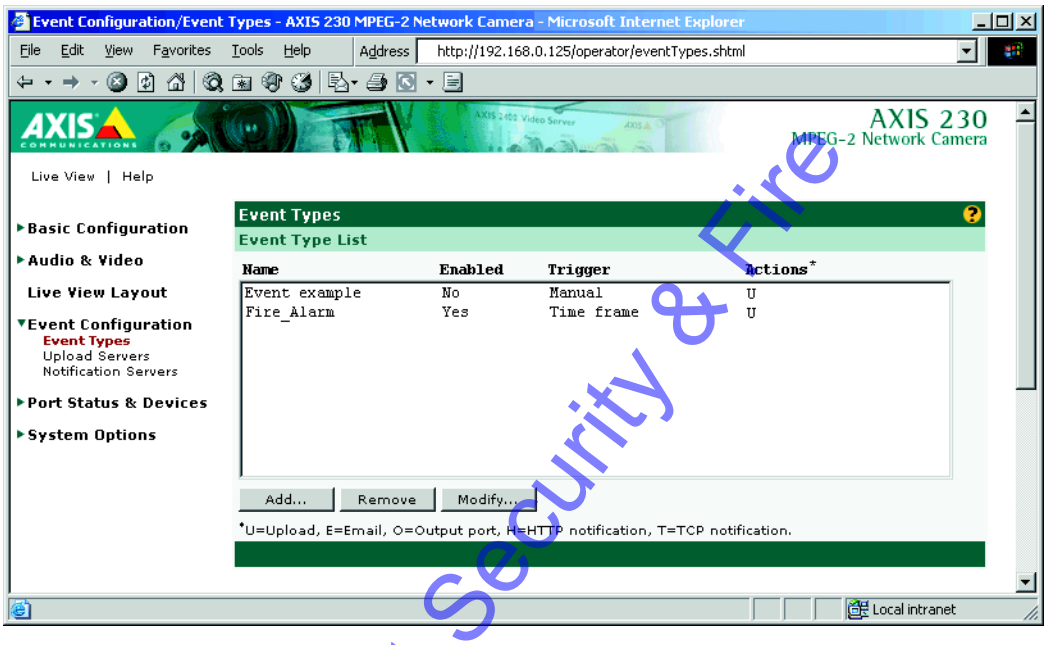
Important!

- Event types that perform uploads should be kept to the minimum required for your application. There is a limit of 3 simultaneous uploads at any one time, although more may be configured.
- Note that when adding, modifying and deleting event types, any other event type that is currently active will be stopped. Stopped event types that have been configured to run for as long as the trigger is active will automatically restart, but others with different configurations will not.

Intelligent Security & Fire

Setting up a new event type

Click the menu link to Event Types. This opens the list of event types as in the example below. The list shows various information about the event types currently configured.



Click the Add button. This launches the *Event Type Setup* dialog. Depending on the event type you require, you will then need to provide some or all of the following information:

General

- Name - Give the event type a suitable name.

Respond to Trigger...

This setting determines when an event can be triggered. The options are:

- Always - the event can be activated by the trigger (see below) at any time
- Only during time frame - a trigger will only start the event during the times specified. Triggers at other times will be ignored. Select the days and set the period's start time and Duration. The Duration may be set up to a maximum of 168 hours. If a Duration of more than 24 hours is required, then only one weekday may be checked. To use two or more trigger time frames of more than 24 hours - two or more event types (one for each time frame) must be configured.
- Never - the event type is disabled and no actions will be performed.

Intelligent Security & Fire

Trigger Type

The trigger type is what starts the event type. The following options are available:

- Input Ports - This describes the states that the 2 inputs must be in before the event is triggered. One or more inputs can be used together, but note that the states for all the inputs used must first be reached before the event is triggered.
- Timer - whole time frame - This option will simply use the times specified in *Respond to Trigger...* described above.
- Timer - periodically - Use this to trigger the event at a certain frequency. Configurable in seconds, minutes or hours. It is also possible to specify the time to commence triggering. Note that this setting also uses the times specified in *Respond to Trigger...*
- Server Boot - This can be used to trigger the event whenever the camera server is started or restarted. A notification of the event would be a suitable action for this trigger type.
- Log Messages - The camera can trigger an event whenever a system event writes an entry to a log file. There are three types of log file; Information, Warning or Critical. Select the level that will trigger the event. Note that the first two alternatives also include messages of a higher importance, so alternative 1 will trigger the event type the most, as it also includes Warning and Critical log messages.
- Manual Trigger - This option makes use of buttons displayed on the Live View page, which are used to start or stop the event manually.
- Audio - This option triggers the event when the selected audio level rises or falls (determined by the Active/Inactive setting) above/below a level defined as -20 dB below the clip level. The green Audio LED indicator is lit in the interval -20dB and 0dB. See also *Audio Settings*, on page 54.

When Triggered...

These settings describe the actions to take when the event type is triggered. One or more actions may be selected.

- Upload to FTP server - Select the FTP server to upload images to. Note that FTP servers must first be configured in *Upload Servers*. See page 25.
  - Upload for - Specify the total time to upload the recording. Configurable in seconds, minutes or hours. This can be used to continue the upload even after the event has ended.
  - Upload as long as trigger is active - This option will terminate the upload as soon as the trigger is no longer active.
  - Split upload into - Use this to split a long video sequence into several shorter sequences. Configurable in seconds, minutes or hours. This is recommended if there is likely to be recordings longer than 30 minutes in duration. The AXIS 230 can easily handle video files of more than 30 minutes, but these may cause problems for some older types of FTP server, due to the large file sizes involved.

Intelligent Security & Fire

- Pre-trigger recording time up to - The AXIS 230 can save recorded sequences that originate from the time immediately preceding the trigger. This can be very useful when checking to see what happened to cause the trigger. The part of the buffer not used for pre-trigger recording is automatically used for post-trigger recording. This is useful in ensuring that there is no video lost during the short time it takes to complete the connection to the FTP upload server.

Notes:
- Exactly how much pre-trigger recording will be produced depends on the quality level setting. Lowering the quality levels for video and audio will increase the duration of the recording.
- When the event is triggered, the pre-trigger recording is uploaded first. The rest of the recording will then follow, although prevailing conditions may result in some images being dropped.
- A high-quality video stream will occupy more of the internal memory and thus shorten the duration of the recording. As pre- and post-trigger FTP uploads have a higher priority, if the network load is heavy, the quality of Live view may suffer.
- Note that as the pre- and post-trigger buffer is always of a fixed size - the more pre-trigger recording is specified, the less will be available for post-trigger recording.
- In the case of overlapping events, the buffer will be locked by the first event, as this has higher priority. The buffer will be available to the second event only when no longer required by the first event.

- Base file name - This name will be used for all of the files saved. If suffixes are also used, the file name will take the form filename_suffix.
- Add suffix - Add either a date/time suffix, a sequence number (with or without a maximum value), or select Overwrite. This last option will save one file only and will constantly overwrite it, whereas using sequential numbering with a maximum will overwrite the first file as soon as the last file is written.

- Activate output port - This box must be checked to enable the use of the output port. The port is used to control external equipment.
  - Keep active during event - This option allows external equipment to be run/controlled for the entire duration of the event. This might be necessary to e.g. keep extra lighting on while saving/uploading a video sequence.
  - Keep active for - Specify a fixed length of time the port will be active for.

Important!

Please keep in mind that the output port can be controlled by more than one event type. This may mean that the port is the “wrong” state if one or more event types that activate the port are triggered one after the other. Using more than one event type to control the output is not recommended.

Intelligent Security & Fire

- Send email notification to - Check this box to enable the sending of email to notify recipients of events. Enter the email address(es) in the field provided. Multiple addresses are separated by commas (,). To add your own text, check the Include text box and enter your text. Note that a mail server must be configured in the SMTP network settings.

- Send HTTP notification - This method sends a notification to an HTTP server. Select the name of the server. Note that the destination server must first be configured in Notification Servers. See the following page.

- Send TCP notification - This method sends a TCP/IP notification. The destination server must also first be configured in Notification Servers.

Click OK to save the event type setup.

Upload Servers

Clicking this link will open the list of FTP servers currently configured in the camera. The listing shows the name and address of the server, as well as the upload path and user name.

Adding an Upload Server

Click the Add button. This opens the *Upload Server Setup* dialog. The following information should then be provided for the new server.

- Name - This can be any descriptive name you like.
- Network address - Enter the IP address or host name of the FTP server. To use a host name, a DNS server must be specified in the TCP/IP network settings.
- Upload path - Specify the path to the directory where the uploaded images will be stored. If this directory does not already exist on the FTP server, there will be an error message when uploading.
- Additional information - In this field you can add extra information about the server. For example, if the saved video files can also be accessed via a UNC address (e.g. \\video\file1.mpeg), you could add text providing this address. This information will be included in email sent by events that use this server.
- The user name and password you use to log on to the server.

When finished, you can test the setup by clicking the Connect button. The results of the connection test will then be displayed in a message box.

Intelligent Security & Fire

Notification Servers

To allow your event types to send HTTP and TCP notifications, the necessary servers must first be configured. The Notification Server list shows the servers currently configured. These servers are shown as the alternatives when selecting this type of notification in the event type setup, as described in the preceding section.

Notification normally requires some sort of script to be located on the destination server. This script reads the parameters sent in the notification and then performs some sort of action.

Note that event notification server settings have nothing to do with the change of IP address notification settings.

The following information should be provided for an HTTP notification server:

- Name - This can be any name you like.
- URL - In this field you should provide the IP or host address of the server, the path to your script, and finally, the name of the script. For example: http://server/path_to_script/script.cgi
- Custom parameters - Enter your own text here. See also below.
- User name/password - If you need to supply a user name and password to access the HTTP server, provide these here.
- Proxy/Proxy port - If you must pass a proxy server to access the HTTP server, provide the server's network address and the port used for access.
- Proxy user name/password - The proxy server may require a user name and password.
- Retry count - If the connection attempt fails, enter the number of times to retry.
- Message - Enter your own text here. This will be displayed in the notification.

This is then what is actually included when the HTTP notification is sent:

http://server/path/script.cgi?Eventname=MyEvent&Message=MyMessage&Custom

For the Custom Parameters field the following should be noted:

- The field must be named as a parameter for it to work.
  For example: http://servername/.....&CustomParameter=MyTextHere.
- The field must be manually URL-encoded. This means that to use special characters, these must be coded and not simply typed. For example, to include a blank space, type %20 instead. The equal sign (=) can be typed directly.

Intelligent Security & Fire

The following information should be provided for a TCP notification server:

- Name - This can be any descriptive name you like.
- Network address - Provide the address of the server here. This may be an IP address or a host name. Note that to use a host name, a DNS server must be configured in the TCP/IP network settings.
- Port - Enter the port number used for accessing the TCP host.
- Retry count - If the connection attempt fails, enter the number of times to retry.
- Message - Enter your own text here. This will be displayed in the notification.

Click OK to save the notification server settings.

Port Status & Devices

Port Status

Clicking this link displays a list showing the status for the 2 inputs and 1 output. The inputs cannot be configured here - this must be done from the System options, which requires administrator access.

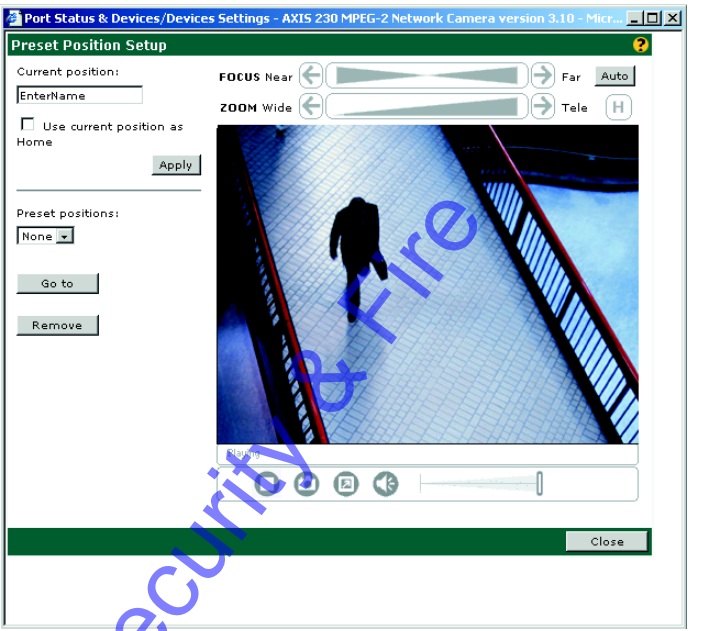
Devices

This section allows you to configure and use Pan/Tilt devices with your AXIS 230. Click the Modify button to open a new window allowing you to create or edit preset positions. Note that Pan/Tilt devices can only be added by the product administrator(s).

Intelligent Security & Fire

Preset position setup - Zoom only

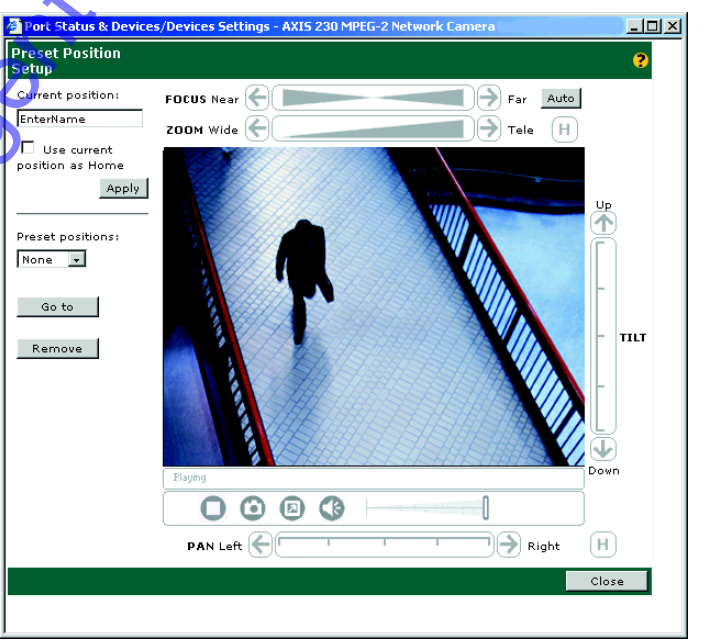
To add a new preset position for the zoom function, zoom the camera to the required magnification and then enter a descriptive name in the *Current Position* field and click Apply. To set a position as Home, check the box provided when that position is current. It is possible to go directly to the Home position from any other position - simply by clicking the H button. To remove a preset position, select it from the drop-down list and click Remove.



Preset position setup - Pan, Tilt & Zoom

To be able to pan and tilt the camera, a Pan/Tilt device and its driver must be added to the camera. The interface will then automatically provide pan and tilt bars. To add a new preset position for all 3 functions, use the controls to steer the camera so that it points to the desired position, and zoom and focus as required. Then add the preset as described above.

Please note that the selected driver will determine the actual layout.



Intelligent Security & Fire

The System Options

This section lists and describes the administration tools used for the general configuration of the AXIS 230 - the System Options. The topics covered are, for example, network settings, date and time settings, users, etc. For information on general usage and how to set up event types, etc., please see *Operating the AXIS 230,* on page 15.

The product cannot be configured before it is installed. If you have not yet completed the installation, please refer to *Installing the AXIS 230,* on page 11.

Only the product administrator(s) can access these settings.

Important Notes!

- The default password (*pass*) for the pre-configured user (*root*) should be changed as soon as possible. Until this has been done, the security features in the product will not be enabled. Furthermore, all Axis products are shipped with the same password by default. For further information, refer to *Users,* on page 30.
- When accessing the AXIS 230 for the first time, you will not be required to log in.
- Javascript must be enabled in your browser for the AXIS 230 Web-based interface to work.

Accessing The System Options

The System Options can be used for configuring the AXIS 230 at any time. Follow the instructions below to access the System Options from your browser:

1. Start your browser and enter the IP address of the AXIS 230 in the address field, for example:

   ```
   http://192.168.0.90
   ```

2. The first time the product is accessed there will be no need to log in. After the Live View page opens, click on the Setup link and then select the item to configure from the System Options.

The system is configured and modified directly from these pages. This can be done from any computer on the network that can access the unit.

Note: Online help is stored internally in the AXIS 230 and is available from the pages in the Web interface. Containing comprehensive details on all product parameters, the on-line help is your first point of reference when configuring and managing the unit.

Intelligent Security & Fire

System Options Overview

The table below provides a brief overview of the System Options. Each section is explained in more detail in the pages that follow.

Administration	Description
Security - Users	Create and delete users and passwords, and modify the Administrator's password.
Security - Firewall Settings	Protect your AXIS 230 against unauthorized access, using the built-in firewall. Allowed IP addresses and protocols can be specified.
Date & Time	Set the system time, manually or automatically.
Network - TCP/IP Settings	Configure TCP/IP settings, enable BOOTP/DHCP and restrict bandwidth.
Network - SMTP (email) Settings	Configure SMTP-settings for sending e-mail messages notifying recipients of recordings, error messages, system messages, etc.
Network - RTP (multicast) settings	Enable and configure multicast IP addresses and ports.
Ports & Devices - I/O Ports	Enable and configure the 2 inputs and 1 output.
Ports & Devices - RS-232 & RS-485	Configure the COM-ports for Generic TCP/IP, Generic HTTP or for a Pan Tilt device.
Maintenance	Provides tools for restarting the camera and for resetting to the factory default settings.
Support - Overview	Provides links to various types of useful information, including how to contact Axis support services.
Support - Logs & Reports	Contains links to various log files and reports.
Support - About	Displays information about the development of the product.

Users

To prevent any unauthorized use of the product, the AXIS 230 supports multi-level and multi-user password protected access. A maximum of 20 users can be defined. An *Administrator* has unrestricted access to the product's administration tools and can determine the registration and rights for all other users.

The Users List displays all of the users currently defined. The administrator user name (*root)* is permanent and cannot be deleted. The default password (*pass)*, however, can and should be changed.

Important!

- Note that if the root password is not changed, then the *Enable anonymous viewer login* checkbox will have no effect, checked or not.
- The *Enable anonymous viewer login* checkbox will, after the root password has been changed, be disabled by default.
- All Axis products are shipped with the same default Administrator password.
- Changing the root password and, later, changing it back to *pass* will return the security function to its original state.

Intelligent Security & Fire

Adding Users

Click Add to add a new user. The following fields must then be completed:

- User Name - Must contain at least one, but not more than fourteen characters.
- Password - Must contain at least one, but not more than eight characters.
- Confirm Password - Repeat the above password here.

User Group - Check the appropriate box to define the access rights and privileges for the new user, where the level of access can be described as follows:

- Viewer - Provides the lowest level of access, which only allows the user to see live images. If the controls for a PTZ unit and/or the Trigger Event button are displayed on the application page, then a user with viewing rights will also be able to use these.
- Operator - An Operator has access to all of the settings not included in the System Options, that is, he/she can add and edit settings for event types, upload servers, audio and video, etc.
- Administrator - An Administrator has unrestricted access to the whole camera and can determine the registration of all other users.

After making the settings for the new user, click the OK button.

Editing and Deleting Users

To edit or delete a user, highlight the name in the User list and click the Modify or Delete button.

Firewall Settings

The built-in firewall protects the AXIS 230 against unauthorized access. To restrict access, add IP addresses to the list of allowed addresses - other addresses will not be permitted access.

Enable/Disable Firewall - Click this button to enable or disable the firewall function.

Allowed IP Addresses - This list box shows the currently configured IP addresses.

Adding Allowed IP Addresses

IP Address - Add a single IP address or a whole range of addresses. This last option can be useful if you have a large number of IP addresses that all need access to the camera. To add a range of addresses, type e.g. 192.168.0.* This will add all the addresses in the range 192.168.0.0 to 192.168.0.255. Up to 256 allowed IP addresses can be specified.

Intelligent Security & Fire

Allowed Ports - Check the boxes for the protocols that the user (IP address) will be allowed to use to access the camera. These can be FTP and/or HTTP. If you have particular requirements concerning which ports access will be allowed on, enter these in the Port range fields. To allow access via HTTP, the port value here must correspond to the value set on the *TCP/IP Network Settings* page. If this is set to some other value than 80 (the default setting), then this value must be added manually in this field. If the setting on the Network Settings page is 80, then nothing needs to be configured here.

After adding the above information click the OK button to save the changes.

Note: If accessing the AXIS 230 via a proxy server, the proxy server's IP address must be added to the list of allowed IP numbers.

Deleting and Modifying the Properties for Allowed IP Addresses

To delete an IP address, select it in the list and click the Remove button. To modify an address, select it from the list of allowed addresses, make the necessary changes and then click OK.

Date & Time

Click Date and Time to define the time and date settings for the AXIS 230, either manually or automatically, as described below.

Current Server Time

Shows the current date and time.

New Server Time

Time Zone - Select the time zone where the AXIS 230 is located.

Automatically adjust for daylight saving time changes - Check this box to automatically update the time changes caused by daylight saving.

Synchronize with computer time - Sets the time according to the clock on your computer.

Synchronize with NTP Server - This option will cause the AXIS 230 to update the time from an NTP server every 60 minutes. Specify the NTP server's IP address or DNS name and set the appropriate time zone for your camera's location. Note that if using a DNS name, a DNS server must be configured in the TCP/IP settings.

Set manually - Using this option allows you to manually enter the time and date.

Intelligent Security & Fire

TCP/IP Network Settings

From the Network Settings, configure the TCP/IP network settings as follows:

Automatic IP Configuration

DHCP - Dynamic Host Configuration Protocol (DHCP) is a protocol that lets network administrators centrally manage and automate the assignment of IP addresses in an organization's network. Check the box to allow a DHCP server on the network to assign the IP address.

Important!

> DHCP should only be enabled if you are using IP address change notification, or if your version of DHCP can update a DNS server, which then allows you to access the AXIS 230 by name. If DHCP is enabled and you cannot access the unit, you may have to reset it to the factory default settings (see page 38) and then perform the installation again (see page 11).

BOOTP - Check this box to use BOOTP to automatically assign an IP address. This requires a BOOTP server on your system. BOOTP is enabled by default.

Dynamic IP Address Notification Settings

When the IP address changes by means beyond your control, for example, by DHCP, you can choose to be notified of the change via HTTP, FTP or SMTP. Click the icon to display, edit and refine the settings for address notification.

Referring to the table below, configure the dynamic IP address notification settings.

Parameter	Description
HTTP	Enabling HTTP means the camera will send an HTTP GET request to the specified URL. This can then easily be taken care of by a designated cgi-script, which registers the request by some means. Custom parameters can be used by entering them in the field provided. The fields User Name and Password, should be used if the script is password protected. If you need to pass a proxy server to connect to the URL for the host, provide your user information in the relevant fields.
SMTP	Enabling SMTP will send an email notification of any change in IP address. Enter the recipient's address and a sender's address, as well as any text you want to appear in the subject of the email. Note that you must configure the mail server under Network Settings.
FTP	Saves a notification file on an FTP server. Provide the connection details for the server and your user name and password. If there is a firewall between the camera and the FTP server, it is recommended that Passive Mode is enabled. There are 3 levels of TXT Type to choose from; Short - the IP address only; Extended - multi-line file; and HTML - contains the same information as Extended, but includes HTML tags. See also the On-line help for more information.
TXT Field	Specify your own text to include in the notification.

Intelligent Security & Fire

Manual IP Configuration

IP Address - Specify a unique IP address for your camera, to establish communication with your network. Written as four numbers separated by periods, each number in the address must be in the range 0 - 255. For example: 192.168.0.125

Note: IP addresses can be assigned at random within isolated networks, provided that each given address is unique. To avoid unnecessary clashes, it is strongly recommended that you contact your network administrator prior to assigning an IP address for your product.

Default Router - Specify the default router (Gateway) used for connecting to other networks and network segments.

Subnet Mask - Specify the subnet mask for the subnet the AXIS 230 is located on.

Host Name - The host name entered here will be used in email sent by the AXIS 230, and in the unit's log files. If the AXIS 230 uses a DNS name on the network, it can be a good idea to use the same name for the host name and the DNS name.

DNS

Domain Name - Enter the name of the domain your AXIS 230 belongs to.

Primary DNS Server - Enter the IP address of the primary DNS server. This server provides the translation of domain names to IP addresses on your network.

Secondary DNS Server - This is used if the primary DNS server is unavailable.

HTTP

Port number - Enter the HTTP port the AXIS 230 will use. The default setting is 80. Alternatively, any port in the range 1024-65535 may be used, but check first with your system administrator before changing the default setting. See also the special considerations concerning the firewall settings, on page 31.

Network Traffic

This can be used to change the network speed for your camera. Normally, there is no need to use anything other than Auto-negotiate, which will automatically select the correct media type. However, if you are using a switch or similar device on your network and need to specify the media type, then this can be done by selecting the correct type from the drop-down list.

Intelligent Security & Fire

SMTP (email) Network Settings

The AXIS 230 can be configured to send event and error email messages to predefined addresses.

Primary mail server - Enter the name or IP address of the server providing your mail facilities. Note that to use a host name, a DNS server must be specified in the TCP/IP network settings.

Secondary mail server - Enter the name or IP address of a secondary mail server. This will be used if the primary mail server is unavailable.

Send test email to - test the setup by clicking the Send button.

RTP (Multicast) Settings

When switching to providing multicast content on the network, there will be no difference in the video stream when compared to ordinary unicasting. The web page containing the content from the AXIS 230 will function exactly as before, and viewers will not experience any change.

To provide multicast broadcasts to multiple viewers, various settings may need to be made. Most importantly, the box “Enable multicast” must be checked.

The other multicast settings concern the IP addresses and port numbers to use for the audio and video streams. If the IP addresses for the two streams are the same, then the ports must be different. Inversely, when using different IP addresses, then the ports can be identical. Note that viewers do not need to know these IP addresses.

The IP addresses used for multicasting audio and video streams should always be selected from within certain specific ranges. The AXIS 230 has been pre-configured with addresses from these ranges, and these should not normally need to be changed. Please contact your network administrator if you have special requirements.

The final multicast setting is the Time to live value. If IP packets (i.e data) fail to get delivered to their destination within a reasonable length of time (which could be for various reasons), this setting tells network routers when to discard the packet. The value is usually measured in "hops", i.e. the number of network routers that can be passed before the packet arrives at its destination or is dropped.

Important!

Note that some network routers may need to be configured to allow RTP traffic.

Intelligent Security & Fire

Ports & Devices

IO Ports

This page allows configuration of the two inputs and one output supported by the AXIS 230. Ports can be given descriptive names, and their *Normal state* can be configured.

The normal state describes the inactive state for the port. It is also an indication of the function of the connected equipment and how it is activated. For example, if the activation circuit in a door switch connected to an input is normally closed, this means that as long as the door is closed then the state is also closed (inactive). When the door is opened the door sensor will be active and the input will no longer be in its normal state. This is how events based on external equipment are triggered.

Thus, in the I/O port list, if the Normal state for an input is set as *Open*, but the Current state is shown as *Closed*, then the port has been activated, and vice versa.

Important!

Please note that some external devices may behave incorrectly in the event of an error condition, e.g. a power cut.

COM Ports RS-232/RS-485

The COM1 port on the AXIS 230 is accessed via the terminal block (RS-485), and COM2 is via the 9-pin D-SUB serial connector. Both are found on the rear of the unit. Select the port from the links in the main menu.

Devices (Pan/Tilt devices, etc) connected to the COM-ports on the AXIS 230 can be controlled via Generic TCP/IP or Generic HTTP, or in the case of Pan/Tilt devices, by a specific driver for the unit being used. Settings are managed and configured directly from the user interface.

Select the port to configure and then choose the Usage for the port, whereupon the relevant settings will be displayed. To make device-specific settings for a Pan/Tilt device, click the Modify button.

For detailed listings of all of the available settings for each mode, the supported Pan/Tilt devices, as well as more information about the different interface modes and pinout info, please the online help, available from the setup pages. See also *Unit Connections,* on page 49.

Intelligent Security & Fire

Maintenance

This section provides tools for the following:

- Restart - Clicking this button will restart the AXIS 230.
- Restore - This button will reset the camera to its factory default settings. Once this has been done, many of the unit's parameters will need to be re-configured. The only settings saved are the IP address, the default router and the subnet mask. See also, on page 38, the description of how to reset to the factory default settings using the Reset button on the rear of the camera.

Support - Logs & Reports

This section of the System Options provides various log files and reports, which may be useful when troubleshooting or when contacting the Axis support services. The logs can be used as triggers for event types. The following are available:

- The Information Log - This log simply records what happens in the camera. It registers when events occur, when the camera is restarted, etc.
- The Warning Log - This log will also include information about errors in the camera that may prevent optimum performance.
- The Critical Log - Registers serious errors that should be rectified as soon as possible.
- The Combined Log - All three logs are shown in one file.

As well as the log files, the following are also available:

- The Server Report - The Server Report displays a listing of important information about the AXIS 230. If you need to contact the Axis Support desk for help with a problem, please include this report with your query.
- The Parameter List - This link displays a listing of all of the AXIS 230's parameters and their current settings. This list should also be included when requesting help from the support desk.

Intelligent Security & Fire

The Factory Default Settings

In certain circumstances, it may be necessary to reinstate the Factory Default settings for your AXIS 230. This is performed in one of two ways:

- By clicking the Restore button from the Maintenance page under System Options. This action will reset most of the unit's parameters but will save the IP-address, the Subnet mask and the Default Router.
- By pressing the Reset button, located on the rear panel. This option will reset ALL the parameters currently configured in the unit, i.e. network settings, events, etc.

Follow the instructions below to reinstate the product factory default settings using the Reset button:

1. Switch off the AXIS 230 by disconnecting the power supply.
2. Press and hold the Reset button, and reconnect the power.
3. Keep the button pressed until the Status Indicator displays *yellow* (note that this may take up to 15 seconds), then release the button. When the Status Indicator displays *green* (which can take up to several minutes) the AXIS 230 will then have been reset to its original factory default settings.

Intelligent Security & Fire

Appendix A - Troubleshooting

This appendix provides useful information to help you to resolve any difficulty you might have with your AXIS 230. Symptoms, possible causes and remedial actions are provided in a quick reference table.

Checking the Firmware

One of your first actions when attempting to solve a problem should be to check the firmware version currently installed. An updated version may contain a correction that fixes your particular problem. For more information, please see *Updating the Firmware,* on page 43.

Support

Should you require any technical assistance, please contact your Axis reseller. If your questions cannot be answered immediately, your reseller will forward your queries through the appropriate channels to ensure a rapid response.

If you are connected to the Internet, you can:

- Download user documentation and firmware updates
- Find answers to resolved problems in the FAQ database. Search by product, category, or phrases.
- Report problems to Axis support staff by logging in to your private support area

Visit the Axis Support Web at www.axis.com/techsup/

Server Report

The server report contains important information about the server and its software, as well as a list of the current parameters. Click the link provided on the Support Overview page.

Viewing the Log Files

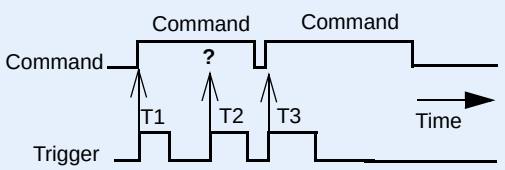
The AXIS 230 log files record events within the unit and can prove useful when attempting to resolve any problems that might occur. Please see *Support - Logs & Reports,* on page 37.

Intelligent Security & Fire

Symptoms, Possible Causes and Remedial Actions

Symptoms	Possible causes	Remedial actions
The AXIS 230 cannot be installed, or cannot be accessed from a browser after installation.	The IP address is already being used by another device.	Run Ping (as described below) and follow the appropriate recommendations.
	The IP address used during installation is not valid on your subnet.	Run Ping. If you get "Destination host unreachable" or similar, the diagnosis is probably correct. In Windows, check that the IP address for your AXIS 230 is on the same subnet as your workstation. Exactly how this is done varies from one version of Windows to another. See Windows' help for more information. If the AXIS 230 and your workstation are on different subnets, you will not be able to set the IP address. Contact your network administrator.
	The IP address has changed.	1) Move the AXIS 230 to an isolated network or to one with no DHCP or BOOTP server. Set the IP address again, using the ARP command. 2) Access the unit and disable BOOTP and DHCP in the TCP/IP settings. Return the unit to the main network. The unit now has a fixed IP address that will not change. 3) As an alternative to 2), if dynamic IP address via DHCP or BOOTP is required, select the required service and then configure IP address change notification from the network settings. Return the unit to the main network. The unit will now have a dynamic IP address, but will notify you if the address changes.
	Other networking problems.	Test the network cable by connecting it to some other network device and then Pinging that device from your workstation. Test the unit's network interface by connecting a local computer to the AXIS 230, using a standard network cable. A crossover cable is not required.
The Power indicator is not constantly lit.	Faulty power supply.	Verify that you are using an Axis PS-K power supply.
The Network indicator displays red.	No network connection or faulty cabling.	See *Other networking problems*, above.
The Status indicator slowly flashes red.	The flash upgrade process has failed.	See the Emergency Recovery Procedure on page 43.
The AXIS 230 works locally, but not externally.	Firewall protection.	Check the Internet firewall with your system administrator.
	Default routers required.	Check if you need to configure the default router settings.
No video.	Display incorrectly configured on workstation.	In Display Properties, adjust the color settings to at least 16-bit color. If running more than one video stream, 32-bit color must be used.

Intelligent Security & Fire

Symptoms	Possible causes	Remedial actions
Slow video	Outdated drivers for graphics card.	Obtain and install the latest device driver for your graphics card from the manufacturer's web site. Also check that DirectDraw acceleration is enabled. This can be done by running the program DxDiag.exe (click Start - Run and then type dxdiag.exe) Check on the Display tab that DirectDraw acceleration is enabled.
	Another application is using DirectDraw acceleration, making this unavailable to the AXIS 230.	Close the other application, and then re-open the AXIS 230's Live View page. Examples of other applications that use DirectDraw acceleration are: video conferencing software, Web TV, video playback software and video editing software.
	Insufficient free memory on graphics card for using the hardware acceleration capabilities.	Lower the resolution/color depth for the monitor. Right-click on the desktop and select Properties - Settings.
Poor quality video (image hopping, etc.), wrong image format (b/w, inverted, etc.)	Outdated drivers for graphics card.	See "Slow video" above.
No audio / poor audio.	Faulty connection to external mic or audio input device. Error in power supply to external microphone.	Check connections. If the audio LED flashes or is steady green, then audio is reaching the MPEG decoder in the AXIS 230 and is included in the stream.
	Incorrect settings.	Check that the correct input is selected. Check the input sensitivity. If the audio LED flashes or is steady green, then audio is reaching the MPEG decoder in the AXIS 230 and is included in the stream.
	Error in client.	Check the settings for the client PC's sound card. If audio is weak or distorted, check the master gain setting in the AXIS 230.
	Outdated drivers for sound card.	Check that you are using the latest device driver for your sound card. Check the manufacturer's web site for new drivers.
Triggering difficulties with programming scripts.	Unable to trigger on both positive and negative transitions of the Control Button and/or I/O ports (double-edged triggering).	Repetitive trigger conditions that occur in quick succession can be missed. This is because the command initiated by the first trigger event may not have been fully executed before the second event starts. This scenario is demonstrated in the illustration below:  This feature has particular significance when using commands that take a relatively long time to process, e.g. mail or FTP, especially if they are transmitting a pre/post alarm buffer.

Note: If you still have a problem after reading this information, please contact your reseller or visit the Axis Support Web at www.axis.com/techsup/

Intelligent Security & Fire

Pinging Your IP Address

By sending a packet to the specified address and waiting for a reply, the Ping utility can determine whether a specific IP address is accessible. It also provides a useful method for confirming addressing conflicts with your AXIS 230 on the network.

Follow the instructions below to ping your unit:

1. Start a Command window and type **`ping x.x.x.x`**, where **`x.x.x.x`** is the IP address of the AXIS 230.
2. If you receive the reply `destination host unreachable`, then the AXIS 230 is not accessible on your subnet. You must obtain a new IP address and reinstall the unit.

If this does not solve the problem, disconnect the AXIS 230 from the network and run Ping again. See the table below for an interpretation of the results.

Ping Reply	Interpretation and recommendation
Reply from <IP address>: bytes = 32; time = 10 ms.....	The IP address is already in use and cannot be used again. You must obtain a new IP address.
Request timed out	This IP address is not used and is available for use with your AXIS 230. If you already installed the unit using this IP address, the installation may have failed. Reinstall the unit. Also check all cabling.

Intelligent Security & Fire

Appendix B - Updating the Firmware

The AXIS 230 firmware is stored in Flash memory. This memory is provided by a silicon chip that, just like any other ROM device, retains data content even after power is removed. Flash memory is unique because it allows its data to be erased and re-written. This means firmware upgrades can be installed as they become available - without having to replace any parts. New firmware is simply loaded into the AXIS 230 over the network.

The latest version of the AXIS 230 firmware is available free of charge from the Axis web site at www.axis.com

Update via FTP

The AXIS 230 Flash memory is updated over the network using FTP. See the detailed instructions supplied with each new firmware release.

Important!

- Always read the instructions provided with each new release, before updating the firmware.
- Upgrading normally takes between 30 seconds and 10 minutes, although it can take longer. After starting the process, you should always wait at least 20 minutes before power-cycling the AXIS 230 - even if you suspect the procedure has failed.
- In controlled environments, flash memory updates provide a very safe way of updating the firmware. However, flash products can become damaged if the update is not performed correctly. Your dealer reserves the right to charge for any repair attributable to faulty updating by the user.

Emergency Recovery Procedure

If power or the network connection to the AXIS 230 is lost during the upgrade, the process will fail and the unit will become unresponsive. A flashing red Status LED indicates a failed upgrade. To recover the unit, follow the steps below. The serial number is found on the label on the product's casing.

1. Unix/Linux - From the command line type the following:
   arp -s <IP address of AXIS 230> <Serial number> temp
   ping -s 408 <IP address of AXIS 230>

   Windows - From a command/DOS prompt type the following:
   arp -s <IP address of AXIS 230> <Serial number>
   ping -l 408 -t <IP address of AXIS 230>
2. If the unit does not reply within a few seconds, restart it and wait for a reply. Press CTRL+C to exit ping.

Intelligent Security & Fire

3. Open a browser and type in the IP address of the AXIS 230. In the page that appears, use the Browse button to select the upgrade file to use, e.g. axis230.bin. Then hit the Load button to restart the upgrade process.
4. After the upgrade has completed (1-10 minutes), the unit will automatically restart and show a steady green on the Power and Status LED:s and flashing green or amber on the Network LED.
5. Repeat the arp and ping commands as described above.
6. Open a new browser and enter the unit's IP address.
7. Reconfigure your settings.

If the emergency recovery procedure does not get the AXIS 230 up and running again, please contact the Axis Support Web at www.axis.com/techsup/

Intelligent Security & Fire

Appendix C - Customizing The AXIS 230

Modifying the File System

The Linux-based operating system and flash memory file system make it possible for advanced users and application developers to customize the AXIS 230 by adding additional files to the read-write area of the flash memory.

Important!

- Modification of the flash file system is NOT supported by Axis. In practice, this means that Axis will not answer questions relating to custom script or Web page development, but merely wishes to inform potential application developers of the possibilities afforded by the Linux-based file structure of the AXIS 230.
- When attempting to modify the product, you may inadvertently create a problem that will require you to return the AXIS 230 to its factory default settings. At worst, you may even cause permanent damage to the unit that renders it unusable. Consequently, Axis strongly recommends that inexperienced users DO NOT modify the file system.

Although modification of the file system is not supported, the Axis web at www.axis.com does maintain various documents designed to assist third-party development. These include detailed information such as:

- The Axis Camera API, HTTP-Interface Specification
- Descriptions of useful scripting technologies

Configuration via FTP

As an alternative to configuring the AXIS 230 using a browser, the configuration parameters of your unit can be modified using the File Transfer Protocol (FTP).

FTP is supported by most operating environments and is a useful method for quickly downloading standard pre-configurations to one or more cameras.

Intelligent Security & Fire

Custom Web Pages

The AXIS 230 contains a re-writable flash memory file system that allows some directories and files to be changed by the *root* user, using FTP. This strictly non-supported product functionality, makes it possible for advanced users and application developers to add their own Web pages, scripts, and other files to the Axis product.

Customizing Procedures

The existing web pages are stored in a compressed read-only area of the file system. If you intend to try changing them you must adhere strictly to the instructions provided here and ensure that you DO NOT inadvertently change any files other than those featured in this section. Failure to comply with this notice may render your product unusable.

All files stored in the `/etc/httpd/html` directory are available through the product Web server in the virtual directory `/local/`. The URL to pages in the `/etc/httpd/html` directory is `http://IP/local/<filename>.htm`.

Editing and Storing Your Web page

Follow the instructions below to save your own pages in the AXIS 230:

1. Using an html editor, create your html file and store it on your local PC hard drive.
2. Now use FTP to upload the file to the AXIS 230. Enter the following on the command line:

Example!

```
ftp 192.168.0.125
```

3. Log on as *root*. The default password for *root* is *pass*, but this may have been changed.
4. Change to the correct directory in the AXIS 230 by entering the following command:

```
cd /etc/httpd/html
```

5. For binary storage of files (not absolutely necessary, but good practice), type `bin`.
6. Upload your html file by entering:

```
put <filename.html>
```

7. Start your browser and view the page you uploaded, by entering the following URL in the location/Address field:

```
http://192.168.0.125/local/<filename.html>
```

Intelligent Security & Fire

Example!

```
http://192.168.0.125/local/index.html
```

Your page now appears in your browser.

8. Enter `bye` in the command window to exit FTP.

Note: You can change the html files as and when you like, but remember that the available flash memory is limited.

Using your own file as a New Home Page

Having created and stored your own web pages in the AXIS 230, you can now assign one of these pages as your default home page, as described below:

Caution!

Changing the web pages in the AXIS 230 is not something that should be undertaken lightly. Remember: Axis does not support the personalization of web pages and strongly recommends that inexperienced users DO NOT perform such modifications.

1. In your browser's URL field (address bar) enter the following:
   http://<IP-address>/admin-bin/editcgi.cgi?file=/etc/httpd/conf/boa.conf
   This opens the built-in editor in the AXIS 230 and loads the file boa.conf for editing.
2. Now add the following lines to the end of the file:

   ```
   Alias /index.html /etc/httpd/html/index.html
   Alias / /etc/httpd/html
   ```

   These lines should be added to the file as shown below:

   ```
   # Virtual I/O specific configurations of Boa

   ScriptAlias /axis-cgi/io/virtualinput.cgi /usr/html/axis-cgi/io/virtualinput.cgi
   Alias /index.html /etc/httpd/html/index.html
   Alias / /etc/httpd/html
   ```

3. This creates an alias to your own `index.html` file stored in the `/etc/httpd/html/` directory and redirects access to it. Save the edited `boa.conf` in the camera, by clicking the Save file button. The next time you access the camera your own web page will now be the first page displayed.

Intelligent Security & Fire

After making these changes, you will not be able to automatically access the default index page. Instead you must type in the complete URL to access it:

```
http://IP#/view/index.shtml
```

or, if PTZ is enabled:

```
http://IP#/view/ptzFrame.shtml
```

Note: As an alternative to the above, edit the line starting with `Document Root` so that it points directly to the local directory. After doing this, however, you will then be unable to access the original home pages - so be warned!

Intelligent Security & Fire

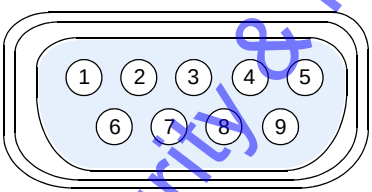
Appendix D - Unit Connections

The D-Sub Connector

The AXIS 230 provides one 9-pin D-sub connector, providing the physical interface for an RS-232 port, used for connecting accessory equipment; such as stand-alone Pan/Tilt devices for the remote positioning of connected video cameras.

A diagram of the RS-232 connector, complete with pin assignment table, is shown below.

Pin	Function
1	CD
2	- RXD
3	- TXD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS
9	RI



The Terminal Block

The terminal block is located on the rear panel and provides the interface to a single transistor output, two digital inputs, an RS-485 interface and GND.

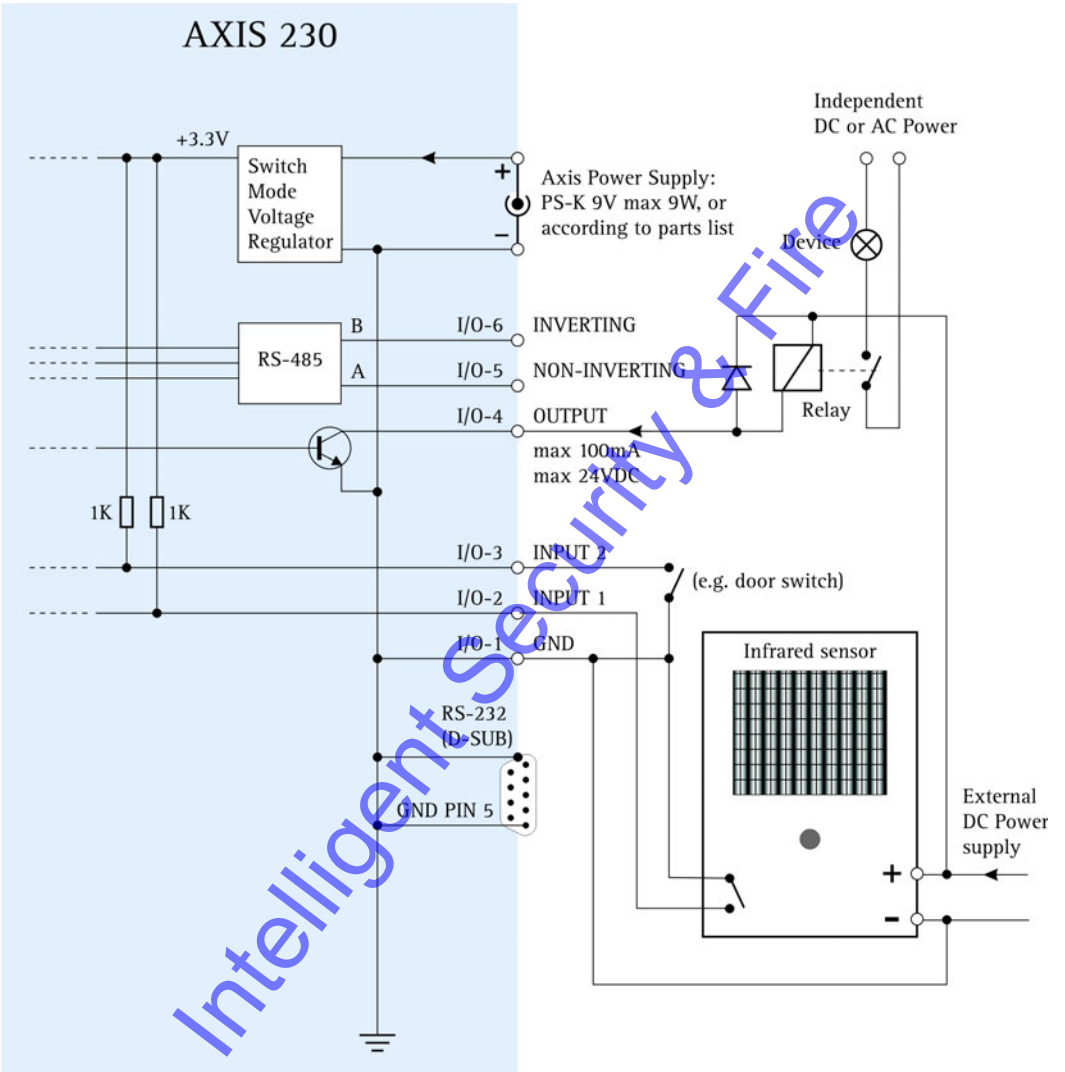
This section describes the pinout, interface support and the control and monitoring functions provided by the terminal block.

Terminal Block Pinout

Pin	Function	Description
1	GND	
2	Digital Input 1	1k internal pull-up. Connect to GND to activate.
3	Digital Input 2	1k internal pull-up. Connect to GND to activate.
4	Digital output	Maximum current sink of 100mA (via logical 0 output.) Handles a maximum voltage of 24V DC, which is grounded at a maximum of 100mA. This output has an open-collector NPN transistor with the emitter connected to pin 1. If used with an external relay, a diode must be connected in parallel with the load, for protection against voltage transients.
5	RS-485-A (non-inverting)	A half-duplex RS-485/422 interface for controlling auxiliary equipment.
6	RS-485-A (inverting)	

Intelligent Security & Fire

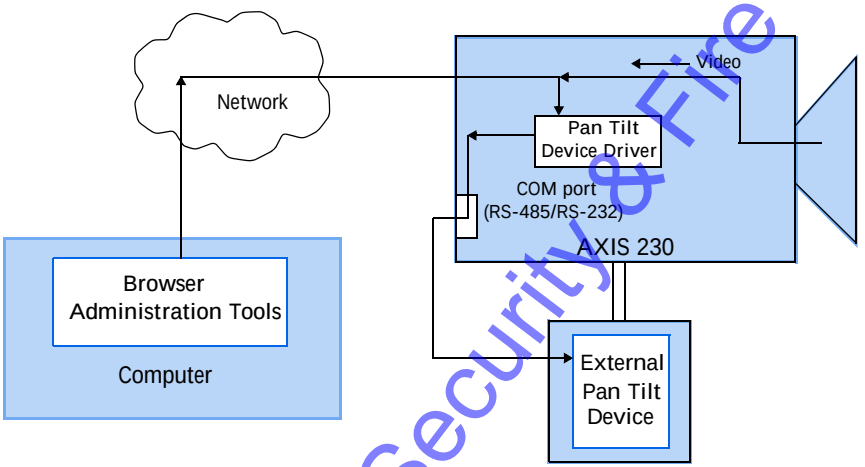
Schematic Diagram - Terminal Connector Block



Connecting Pan/Tilt Devices

The AXIS 230 supports a range of Pan Tilt device drivers. The driver is selected from the *COM Port* settings, which are found under *System options - Ports & Devices*. Please see the online help or www.axis.com for a complete list of supported devices.

The diagram below illustrates how the AXIS 230 connects to your workstation and a Pan Tilt device.



Intelligent Security & Fire

Installation Procedure

1. Attach the Pan/Tilt device to the RS-232 port (serial connector) or the RS-485 port on the Terminal Block, using the appropriate cable.
2. From the AXIS 230 Home Page, click Setup.
3. Under System Options - Ports & Devices - select the port the device is connected to. Then select Pan/Tilt as the Usage for that port.
4. Now select the driver for your Pan/Tilt/Zoom device from the drop-down list. Click Save. To make device-specific settings, click the button provided.
5. You can now configure preset positions for your device from the Devices page, under Port Status & Devices.

Note: Advanced users and application developers can also use the Axis Application Programming Interface and HTTP specification for generic control of pan tilt devices using CGI parameters or a TCP/IP client. Please refer to the Axis Web site for further information.

Controlling and Monitoring

By entering http requests in your browser's URL field, you can:

- drive the transistor output high or low
- monitor the status of the digital inputs

This requires administrator access to the AXIS 230, and thus a user name and password. Log in as *root* and supply the root password (default = *pass*).

Tip!

Developers wishing to create applications incorporating sophisticated alarm conditioning using the transistor output and digital inputs are encouraged to read the Camera API, HTTP-Interface Specification, available from the Axis Web at www.axis.com.

Transistor Output

The output can directly drive a maximum load of 24V DC at 100mA. By connecting additional relay circuitry, heavier loads can be driven.

The transistor output is controlled using HTTP requests, as shown in the following examples:

Example 1: - Set output 1 ON

```
http://server/axis-cgi/io/output.cgi?action=1:/
```

Example 2: - Set two 300ms pulses with 500ms delay between the pulses, on output 1.

```
http://server/axis-cgi/io/output.cgi?action=1:/300\500/300\
```

Example 3: - Wait 1 second before setting output 1 ON.

```
http://server/axis-cgi/io/output.cgi?action=1:1000/
```

Digital Inputs

Two digital inputs allow the AXIS 230 to be configured for device triggered events. For example, by connecting a motion detector to a digital input, it is a relatively simple procedure to trigger an event each time the detector is activated.

Querying the Status of Digital Inputs

The status of the digital inputs can be queried in exactly the same way as the relay output. Simply enter the following URL to query the status of the digital inputs:

Intelligent Security & Fire

Example: - Monitor data on inputs 1 and 2

```
http://server/axis-cgi/io/input.cgi?check=1,2
```

The AXIS 230 then displays the status of the inputs, as follows:

```
Input 1 = 0
Input 2 = 1
```

Intelligent Security & Fire

Appendix E - Audio Settings

The maximum audio level depends on the configuration used.

- Selecting external microphone and high sensitivity input, sets the 0dB level (the maximum level) to 25mVpp.
- Selecting external microphone and low sensitivity input, sets the 0dB level (the maximum level) to 270mVpp.
- Selecting external line input sets the 0dB level (maximum level) to 3.0 Vpp.

The Audio LED remains unlit as long as the audio level is below -20dB, as compared to the maximum audio level, which is defined as 0dB.

The LED turns green when the audio level is between -20dB and 0dB. This is the optimum audio level. The LED turns red if the audio level rises above the clip level (the maximum level), that is, above 0dB.

Generally speaking, normal speech at a distance of 1 meter will, in high sensitivity mode, produce sound levels high enough to light the LED green. When the microphone is set up in a noisy environment, it may be necessary to set the sensitivity to "low," otherwise the clip level will be reached and the sound will become distorted. For very high sound pressure levels, use an external microphone with a controlled output level.

The audio “event" (as used to trigger events) always correlates to if the green LED is lit. By using different input settings, the audio event trigger level can thus be given different values.

The master volume does not affect the maximum levels into the A/D-converter in the camera, nor does it affect the audio input LED or the trigger level for the audio event. The master volume is only a gain factor that changes the already sampled and digitized signal. For this reason it is important that the signal is handled within the correct dynamic range, by changing the sensitivity settings rather than the master volume - otherwise the signal may become distorted due to input overload.

The Master volume can be used to match other PC-produced "wave sounds", since there is no separate volume control for the decoded audio in the PC sound card interface. This means that system sounds in the client computer are affected by the same volume control as the incoming sound from the Axis 230.

Normally, the Audio LED monitors the input level and will show red if the audio input signal is too strong, which will also be apparent as the sound becomes distorted. However, increasing the Master Gain may cause distortion at other levels, which will not be indicated by the Audio LED. For this reason, increasing the Master Gain when the Audio LED shows almost constant green is not recommended.

Intelligent Security & Fire

Appendix F - Technical Specifications

System Requirements - Windows® 2000 or Windows XP (with latest Service Pack.) AGP graphics card with 16 MB video memory and support for DirectDraw®. Use the latest available driver. Internet Explorer 5.5 or higher (with latest Service Pack.) DirectX® (latest version.)

Installation - Physical network connection using RJ-45 twisted pair cable. 10baseT or 100baseTX Fast Ethernet.

Management - Remote configuration and status using Web-based tools.

Video Features - MPEG-2 video compression. Configurable resolution, color and quality levels.

Audio In - One 3.5mm input for stereo or mono microphone, or for line-in stereo or mono signal. The logical port is selected in the web interface.

Stereo microphone input - High sens. Max:-39.0 dBu (25 mVpp)
Stereo microphone input - Low sens. Max:-18.1 dBu (270 mVpp)
Line input - Max:+2.7 dBu (3.0 Vpp)

Supported Network protocols - TCP/IP, HTTP, FTP, SMTP, NTP, ARP, DHCP, BOOTP, RTP

Terminal block connector - 2 digital inputs (max 12 V in) and 1 transistor output (max 24 V, 0.1 A). 1 pin for ground. 2 pins for RS-485 serial communication.

Pre/Post Alarm Buffer - Approximately 15 MB memory for storage of pre/post alarm video.

Serial Connector - One 9-pin D-Sub RS-232, max 115 Kbit/s.

Pan/Tilt - Pan/Tilt support via RS-232 or RS-485 for remote camera control. See www.axis.com or the online help for information about supported devices.

Security - Multi-user and multi-level password protection.

Operating Conditions: - Temp: +5^{o} to +50^{o} C (41^{o} to 122^{o} F). Humidity: 20-80% RH.

Illumination - Min illumination = 0,7 lux (at F1.4 1/60s NTSC or 1/50s PAL) (50IRE) (down to 0.01 lux, depending on shutter speed.) Recommended illumination: 100 to 100.000 lux.

Intelligent Security & Fire

Approvals - EMC

- EN 55024:1998+A1 (CISPR 24:1997+A1.) Applies when using the internal microphone or an external line input, but not when using an external microphone.
- EN61000-6-1:2001
- EN61000-6-2:2001
- EN 55022:1998+A1 Class B (CISPR 22:1997+A1, Class B)
- FCC Part 15, Subpart B, Class B demonstrated by compliance with EN 55022 (CISPR 22)
- EN 61000-3-2:2000
- EN 61000-3-3:1995+A1
- VCCI:2003, Class B, ITE (Japan)
  (CISPR 22:1997+A1, Class B)
- C-Tick mark - according to AS/NZS3548 (equivalent to CISPR 22:1997+A1) (Australia)

Approvals - Safety - EN60950, CSA.

Metrics: - Height: 3.15" (80mm), Width: 2.95" (75mm), Length (without connectors): 6.73" (171mm), Weight: 1.65lb (0.75kg) excluding Power Supply.

Hardware - MPEG-2 compression chip, ETRAX-100LX, 32-bit RISC, 100 MIPS CPU, 32 MB RAM, 4 MB FLASH PROM.

Power - PS-K, (included) 9V DC, 9W. Alternative supply 7-20V DC, min 7W.

Complimentary Software - AXIS Media Control (ActiveX component software for Microsoft Internet Explorer - supplied with the product). AXIS IP Utility - for quick and simple installation. Available from the Axis web site.

File size - The file sizes delivered by the AXIS 230 can be calculated as follows:

$$\frac{(Ba + Bv) \times 1000 \times 60}{8} = \text{file size in bytes/minute}$$

Bv = Bit rate for video (kbit/s), Ba = Bit rate for audio (kbit/s, 0 if not enabled).

Intelligent Security & Fire

Appendix G - Bandwidth

As different networks have different characteristics and different amounts of bandwidth available, the AXIS 230's video and audio settings may need to be adjusted to suit the prevailing conditions.

The Video Quality Level

The video quality level describes how much video data is transferred per second, and can be set in the range 1-7 (lowest to highest). Whether or not you should use the highest available level depends on the answers to a few questions:

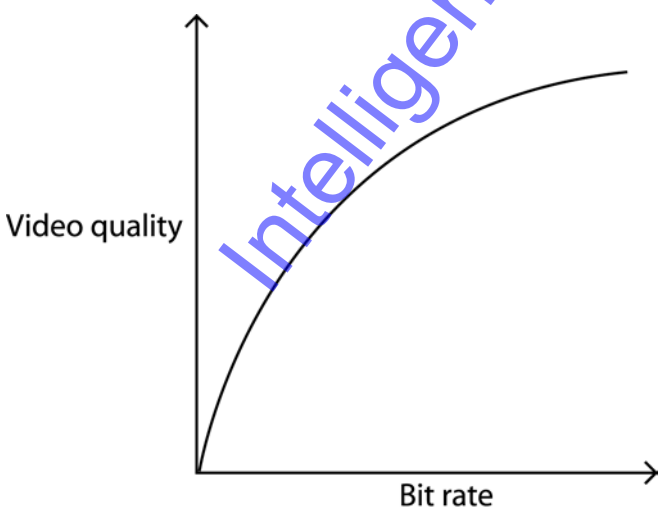
Does your application actually need a video stream at the highest quality? Try viewing the live video stream and uploading MPEG-2 files using several different quality levels.

Are there other bandwidth-dependent services running on the same network? Will the quality level used by the AXIS 230 cause problems for these services?

How many clients are likely to be viewing the video stream at any one time? The maximum number of (unicast) viewing clients on a local area network is 3.

Video Quality vs. Bit Rate

The quality of the video stream in relation to the bit rate is roughly illustrated by the following graph.



Intelligent Security & Fire

Other Considerations

- The MPEG-2 encoder chip in the AXIS 230 is designed for constant video bit rates from 1.0 - 8.0 Mbit/s. The parameter on the encoder chip that controls the video bit rate allows even lower settings, but not at constant bit rates. At low bit rates, the encoder delivers variable bit rates, and the rate is strongly affected by the selected video resolution and image information.
- The video quality level can be set from 1 (low) to 7 (high.) When using the levels 1-3, the bit rate can become variable. The total bandwidth usage is determined by the audio and video quality level and the protocol-specific contribution. Using quality levels lower than 3 may reduce bandwidth usage at the expense of image quality.

The table below shows recommended video quality levels at various resolutions:

Resolution	Unicast	Multicast
4CIF	4-7	4-6
2CIF	3-7	3-6
CIF	3-7	3-6
QCIF	3-7	3-6

- There is a limit of 3 simultaneous uploads at any one time, although the number of event types configured to upload can be greater than 3.
- If installing multiple units on the same network, the bandwidth requirements will be significantly higher.

Intelligent Security & Fire

Index

A
Access from a browser 14
Actions 21
Activate output port 24
Adding
  Allowed IP addresses 31
  Notification servers 26
  Upload servers 25
  Users 30
Additional information - upload servers 25
Administrator - user group 31
Advanced image settings 19
Allowed IP addresses 31
Anonymous viewers 30
Applications 8
Audio - event triggering 23
Audio Equipment 14
Audio In connector 14
Audio settings 20, 54
Automatic IP Configuration 33
AXIS IP Utility 11
AXIS Media Control 13

B
Bandwidth 57
Base file names 24
Brightness 18

C
Camera features 6
Clients 12
COM-Port 36
Configuration
  Event types 21
  Firewall 31
  Network 33
  Notification servers 26
  SMTP 35
  Upload servers 25
  Users 30
Connecting Pan/Tilt devices 51
Connectors 49
Control Applet 13
Critical Log 37
Custom Parameters - HTTP notifications 26
Customizing the camera 45

D
Date & time settings 32
Devices 27
DHCP 33
Digital output 49
DirectX 12
Disconnected Video Sources 17
DNS 34
D-Sub Connector 49

E
Email event notification 25
Emergency recovery 43
Events 21
Events and event types 17
External mic power 20

F
Factory Default Settings 38
Firewall 31
Firmware 39
Focus Near Limit 19
Front panel 9
FTP
  IP address notification 33
  upload servers 25

Intelligent Security & Fire

G
Group of Pictures (GOP) 19

H
Hardware Inventory 10
Home page 47
HTTP
event notification 25
IP address notification 33
notification server 26
port number 34

I
I/O Terminal Block 49
Information Log 37
Input Ports - event triggering 23
Inputs 36
Installation 11
Installing Pan/Tilt devices 51
Internet Explorer 12
IO Ports 36
IP address notification 33
IP addresses - allowed 31
IP Utility 11
IR Illumination 19

K
Keep active during event 24
Keep active for 24

L
Layout - live view 20
Live View 14, 16
Log files 37, 39
Log files - event triggering 23

M
Mail settings 35
Maintenance 37
Manual IP Configuration 34
Manual trigger 23
Master volume 54
Max Digital Zoom 19
Mic input sensitivity 20
Microphones 14
Mirror 19
MPEG-2 13
Multicasting 6, 35

N
Network settings 33
Network Traffic 34
New home page 47
Notification servers 26
NTP Server 32

O
Operation 15
Operator - user group 31
Output 24, 36
Own web pages 46

P
Pan/Tilt 17
Pan/Tilt devices 17, 51
Parameter List 37
Passwords 30
Ping 11
Pinout - I/O connectors 49
Port Status 27
Ports & devices 36
Positional control 17
Preset posistions 28
Pre-trigger recording 24

Q
Quality level 18

R
Rear panel 9
Recommended platform 12
Recovery 43
Reports 37
Resolution 18

Intelligent Security & Fire

Respond to trigger... 22
Restarting the server 37
Restoring the factory default settings 37
Retry count - HTTP notifications 26
Root password 30
RS-232 36
RS-232 serial interface 49
RS-485 36
RTP 35

S
Schematic diagram 50
Sensitivity - microphone setting 14
Server boot - event triggering 23
Server Report 39
Setting up event types 22
Setup Tools 17
Sharpness 18
Shutter speed 18
SMTP
  IP address notification 33
  network settings 35
Source modulation 18
Specifications 55
Splitting uploads 23
Suffixes 24
Support 37, 39
System options 29
System requirements 12

T
TCP
  event notification 25
  notification servers 27
  Port number 32
TCP/IP network settings 33
Technical specifications 55
Terminal block 49
Time Zone 32
Timer - event triggering 23
Transistor output 52
Trigger types 23
Triggers 21
Troubleshooting 39

U
Unicasting 6
Updated firmware 43
Upload servers 25
Uploading to FTP servers 23
User groups 31
Users 30

V
Video bit rate 57
Video quality 57
Video Settings 18
Viewer - user group 31
Volume 20

W
Warning Log 37
When triggered... 23
White Balance 18

Intelligent Security & Fire

Glossary of Terms

ActiveX - A control (or set of rules) used by a browser. ActiveX controls are often downloaded and installed automatically as required.

ARP - Address Resolution Protocol. A protocol for assigning an IP address to a physical device address that is recognized in the local network. The ARP command can be used to set the IP-address for your product.

ARTPEC - Axis Real Time Picture Encoder - used for image compression.

BOOTP - A protocol that can automatically configure a network device (give it an IP address).

CGI - Common Gateway Interface. A set of rules (or a program) that allows a Web Server to communicate with other programs.

DSL - Digital Subscriber Line. A means of transferring data via standard phone lines.

Ethernet - A widely used networking standard.

ETRAX - Axis' own microprocessor.

Firewall - A virtual barrier between a LAN (Local Area Network) and other networks, e.g. the Internet.

Frame Grabber card - Plug-in hardware for "grabbing" images

FTP - File Transfer Protocol. Used for simple transfer of files to and from an ftp-server.

HTML - Hypertext Mark-up Language. Used widely for authoring documents viewed in web browsers.

HTTP - Hypertext Transfer Protocol. The set of rules for exchanging files (text, images, sound, video, and other files) on the World Wide Web.

Intranet - A private network limited to an organization or corporation. Usually closed to external traffic.

IP - Internet-Protocol. See TCP/IP.

IP address (number) - A unique number used by a computer on the network to allow it to be identified and found.

JPEG - A standard image format, used widely for photographs. Also known as JPG.

LAN - A local area network (LAN) is a group of computers and associated devices that typically share common resources within a limited geographical area.

Linux - A popular operating system, that is “open source” and practically free of charge.

Lux - A standard unit for light measurement.

Mbit/s - Megabits per second. A unit for measuring speeds in networks. A LAN might run at 10 or 100 Mbit/s.

NWAY - A network protocol that automatically negotiates the highest possible common transmission speed between two devices.

Ping - A small utility used for sending data packets to network resources to check that they are working and that the network is intact.

PPP - Point-to-Point Protocol. A method allowing one computer to connect to another, usually via a modem over a phone line.

Pre/post alarm image - The images from immediately before and after an alarm.

Protocol - A special set of rules governing how two entities will communicate. Protocols are found at many levels of communication, and there are hardware protocols and software protocols.

RTP - The Real-Time Transport Protocol is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over unicast or multicast network services. RTP combines its data transport with a control protocol (RTCP), making it possible to monitor data delivery for large multicast networks. Both protocols work independently of the underlying Transport layer and Network layer protocols. As a rule, RTP runs on top of the User Datagram Protocol (UDP), although it can use other transport protocols.

SMTP - A common e-mail protocol.

TCP/IP - Transmission Control Protocol/Internet Protocol. A suite of network protocols that determine how data is transmitted. TCP/IP is used on many networks, including the Internet. TCP keeps track of the individual packets of information and IP contains the rules for how the packets are actually sent and received.

UDP - The User Datagram Protocol is a communications protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is also known as UDP/IP.

URL - Uniform Resource Locator. An "address" on the network.

WAN - Wide-Area-Network. Similar to a LAN, but on a larger geographical scale.

Web server - A program on a computer that delivers the resources (usually web pages) requested by the web user (the client).

Intelligent Security & Fire